

Security made simple.

SafeGuard Enterprise
Manuel d'administration

Version du produit : 6.1
Date du document : janvier 2014

Table des matières

1 À propos de SafeGuard Enterprise 6.1....................4
2 Bon usage en matière de sécurité....................6
3 À propos de SafeGuard Management Center....................9
4 Connexion au SafeGuard Management Center....................10
5 Licences....................14
6 Utilisation de plusieurs configurations de base de données....................20
7 Création de la structure organisationnelle....................25
8 Responsables de la sécurité de SafeGuard Enterprise....................35
9 Clés et certificats....................54
10 Ordres de modification du certificat d'entreprise....................67
11 Utilisation de stratégies....................71
12 Utilisation des packages de configuration....................83
13 Authentification au démarrage de SafeGuard....................87
14 Accès administratif aux ordinateurs d'extrémité Windows....................98
15 Listes de comptes de service pour la connexion Windows....................99
16 Utilisateurs de l'authentification au démarrage pour connexion à l'authentification au démarrage SafeGuard.104
17 Paramètres de stratégie....................111
18 Chiffrement du disque....................150
19 Protection de la configuration SafeGuard....................164
20 Utilisation de File Encryption avec File Share....................165
21 SafeGuard Data Exchange....................177
22 Cloud Storage....................187
23 Attribution utilisateur-ordinateur....................193
24 Tokens et cartes à puce....................198
25 Éveil par appel réseau sécurisé (WOL)....................215
26 Options de récupération....................217

27 Restauration d'une installation SafeGuard Management Center en cas de corruption...........245

28 Restauration d'une configuration de base de données corrompue...246

29 Données d'inventaire et d'état..247

30 Rapports...254

31 Planification des tâches..267

32 Gestion des ordinateurs d'extrémité Mac dans SafeGuard Management Center.....................277

33 SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique.............279

34 Événements disponibles pour les rapports...282

35 Codes d'erreur...293

36 Support technique...309

37 Mentions légales..310

1 À propos de SafeGuard Enterprise 6.1

SafeGuard Enterprise assure une protection puissante des données à travers le chiffrement et une authentification supplémentaire à la connexion.

Cette version de SafeGuard Enterprise prend en charge Windows 7 et Windows 8 fonctionnant sur des ordinateurs d'extrémité dotés de BIOS ou d'UEFI.

- Pour les plates-formes BIOS, vous pouvez choisir entre le chiffrement intégral du disque SafeGuard Enterprise et le chiffrement BitLocker géré par SafeGuard Enterprise. La version BIOS est livrée avec le mécanisme de récupération BitLocker original.

  Remarque : si l'authentification au démarrage SafeGuard ou le chiffrement intégral du disque SafeGuard sont mentionnés dans le présent manuel, il font uniquement référence aux ordinateurs d'extrémité Windows 7 avec BIOS.

- Pour les plates-formes UEFI, veuillez utiliser BitLocker géré par SafeGuard Enterprise pour le chiffrement du disque. Pour ces ordinateurs d'extrémité, SafeGuard Enterprise offre des fonctionnalités améliorées de Challenge/Réponse. Retrouvez plus de renseignements sur les versions UEFI prises en charge et sur les limites de la prise en charge du Challenge/Réponse SafeGuard BitLocker dans les Notes de publication disponibles sur http://downloads.sophos.com/readmes/readsgn_61_fra.html.

Remarque : la mention UEFI apparaît de manière explicite à chaque fois qu'elle doit être utilisée.

Le tableau ci-dessous indique quels composants sont disponibles.

	Chiffrement intégral du disque SafeGuard avec authentification au démarrage SafeGuard	Authentification de préinitialisation BitLocker gérée par SafeGuard	Récupération C/R SafeGuard pour l'authentification de préinitialisation BitLocker
Windows 7 BIOS	**OUI**	**OUI**	
Windows 7 UEFI		**OUI**	**OUI**
Windows 8 UEFI		**OUI**	**OUI**
Windows 8 BIOS		**OUI**	
Windows 8.1 UEFI		**OUI**	**OUI**
Windows 8.1 BIOS		**OUI**	

Remarque : la **Récupération C/R SafeGuard pour l'authentification de préinitialisation BitLocker** est uniquement disponible sur les systèmes 64 bits.

Le **Chiffrement intégral du disque SafeGuard avec authentification au démarrage SafeGuard** est le module Sophos permettant de chiffrer les volumes sur les ordinateurs d'extrémité. Il est

livré avec l'authentification de préinitialisation Sophos nommée authentification au démarrage SafeGuard qui prend en charge les options de connexion par cartes à puce, par empreinte digitale et qui offre un mécanisme Challenge/Réponse pour la récupération.

L'**Authentification de préinitialisation BitLocker gérée par SafeGuard** est le composant qui active et gère le moteur de chiffrement BitLocker et l'authentification de préinitialisation BitLocker.

Elle est disponible sur les plates-formes BIOS et UEFI :

- La version UEFI propose également un mécanisme Challenge/Réponse SafeGuard pour la récupération de BitLocker lorsque l'utilisateur oublie son code PIN. La version UEFI peut être utilisée si la plate-forme répond à certaines conditions préalables requises. Par exemple, la version UEFI doit être 2.3.1. Retrouvez plus de renseignements dans les Notes de publication.
- La version BIOS ne propose pas toutes les fonctions de récupération offertes par le mécanisme Challenge / Réponse SafeGuard. Elle sert d'option de secours lorsque les conditions requises à l'utilisation de la version UEFI ne sont pas remplies. Le programme d'installation Sophos vérifie si les conditions requises sont remplies et en cas contraire, il installe automatiquement la version BitLocker sans Challenge/Réponse.

Ordinateurs d'extrémité Mac

Les produits mentionnés ci-dessous sont disponibles pour les ordinateurs d'extrémité Mac. Ils sont également gérés par SafeGuard Enterprise ou communiquent leur rapport d'état à la console d'administration Management Center.

	Sophos SafeGuard File Encryption 6.1	Sophos SafeGuard Disk Encryption 6.1 (FileVault 2) administré par SafeGuard	Sophos SafeGuard Disk Encryption pour Mac 6.0 (envoi de rapport au Management Center)
OS X 10.7	**OUI**		**OUI**
OS X 10.8	**OUI**	**OUI**	**OUI**
OS X 10.9	**OUI**	**OUI**	

Ce manuel fait uniquement référence à la plate-forme Windows. Retrouvez plus d'informations sur les versions Mac dans la documentation produit respective.

2 Bon usage en matière de sécurité

En suivant les étapes simples mentionnées ci-dessous, vous pourrez écarter les risques et conserver les données de votre entreprise sécurisées et protégées à tout moment.

Pour utiliser SafeGuard Enterprise dans un mode conforme à la certification, reportez-vous au *Manuel SafeGuard Enterprise pour une utilisation conforme à la certification.*

Évitez le mode veille

Sur les ordinateurs protégés par Sophos SafeGuard, il est possible que certains individus malintentionnés accèdent aux clés de chiffrement dans certains modes de veille. Tout particulièrement lorsque le système d'exploitation de l'ordinateur n'est pas arrêté correctement et que les processus en tâche de fond restent en cours d'exécution. La protection est renforcée lorsque le système d'exploitation est complètement arrêté ou mis en veille prolongée.

Formez les utilisateurs en conséquence ou considérez la désactivation centrale du mode veille sur les ordinateurs d'extrémité sans surveillance ou qui ne sont pas en cours d'utilisation :

- Évitez le mode veille (attente/veille prolongée) ainsi que le mode de veille Hybride. Le mode de veille Hybride allie la mise en hibernation et la mise en veille. La définition d'un mot de passe supplémentaire après la reprise d'une session n'assure pas de protection complète.

- Évitez de verrouiller les ordinateurs de bureau et de mettre hors tension les moniteurs ou de fermer les couvercles des portables en guide de protection si ce n'est pas suivi par une véritable mise hors tension ou en hibernation. La demande d'un mot de passe supplémentaire après la reprise d'une session ne fournit pas une protection suffisante.

- Arrêtez vos ordinateurs ou mettez-les en hibernation. L'authentification au démarrage SafeGuard est toujours activée jusqu'à la prochaine utilisation de l'ordinateur. Ce dernier est ainsi totalement protégé.

  Remarque : il est important que le fichier de mise en veille prolongée soit sur le volume chiffré. Généralement, il se trouve sur C:\.

  Vous pouvez configurer les paramètres d'alimentation appropriés de manière centralisée à l'aide d'Objets de stratégie de groupe ou localement via la boîte de dialogue **Options d'alimentation** du **Panneau de configuration** de l'ordinateur. Définissez l'action du bouton **Veille** sur **Mettre en veille prolongée** ou **Arrêter**.

Mettez en place d'une stratégie de mot de passe forte

Mettez en place une stratégie de mot de passe forte et imposez des changements de mot de passe à intervalles réguliers, surtout pour la connexion à l'ordinateur d'extrémité.

Les mots de passe ne doivent être partagés avec quiconque ni écrits.

Formez vos utilisateurs pour choisir des mots de passe forts. Un mot de passe fort suit les règles suivantes :

- Il est assez long pour être sûr : il est conseillé d'utiliser au moins 10 caractères.

- Il contient un mélange de lettres (majuscules et minuscules) ainsi que des caractères spéciaux ou des symboles.

- Il ne contient pas de mot ou de nom fréquemment utilisé.
- Il est difficile à deviner mais simple à se rappeler et à saisir correctement.

Ne désactivez pas l'authentification au démarrage SafeGuard

L'authentification au démarrage SafeGuard fournit une protection de connexion supplémentaire sur l'ordinateur d'extrémité. Grâce au chiffrement complet du disque SafeGuard, elle est installée et activée par défaut. Pour une protection complète, ne la désactivez pas.

Protégez-vous contre l'injection de code

L'injection de code, par exemple à travers une attaque par chargement préalable de fichiers DLL, est possible lorsqu'un attaquant parvient à placer du code malveillant (comme des exécutables) dans des répertoires qui peuvent faire l'objet de recherches pour trouver du code légitime par le logiciel de chiffrement Sophos SafeGuard. Pour écarter ce type de menace :

- Installez le middleware chargé par le logiciel de chiffrement, par exemple un middleware de token, dans des répertoires inaccessibles aux attaquants externes. Il s'agit généralement de tous des sous-dossiers des répertoires **Windows** et **Program Files**.
- La variable d'environnement PATH ne doit pas contenir de composants qui pointent vers des dossiers accessibles aux attaquants externes (voir ci-dessus).
- Les utilisateurs standard ne doivent pas avoir de droits d'administration.

Bon usage en matière de chiffrement

- **Assurez-vous qu'une lettre a été attribuée à tous les lecteurs.**

  Seuls les lecteurs auxquels une lettre a été attribuée sont pris en compte pour le chiffrement/déchiffrement du disque. Les lecteurs sans lettre sont susceptibles d'entraîner des fuites de données confidentielles en texte brut.

  Pour écarter ce type de menace : ne permettez pas aux utilisateurs de changer les attributions de lettres au lecteur. Définissez leurs droits utilisateurs en conséquence. Les utilisateurs standard de Windows n'ont pas ce droit par défaut.

- **Appliquez un chiffrement initial rapide avec précaution.**

  Sophos SafeGuard propose le chiffrement initial rapide pour réduire le temps du chiffrement initial des volumes en accédant seulement à l'espace véritablement utilisé. Ce mode conduit à un état moins sécurisé si un volume a été utilisé avant son chiffrement avec SafeGuard Enterprise. À cause de leur architecture, les SSD (Solid State Disks) sont affectés davantage que les disques durs standard. Ce mode est désactivé par défaut. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/113334.aspx.

- **Utilisez seulement l'algorithme AES-256 pour le chiffrement des données.**
- **Utilisez SSL/TLS (SSL version 3 ou supérieure) pour la protection de la communication client/serveur.**

  Retrouvez plus d'informations dans le *Guide d'installation de SafeGuard Enterprise*.

- **Empêchez toute désinstallation.**

Pour renforcer la protection des ordinateurs d'extrémité, vous pouvez empêcher la désinstallation locale de Sophos SafeGuard dans une stratégie **Paramètres de machine spécifiques**. Définissez l'option **Désinstallation autorisée** sur **Non** et déployez cette stratégie sur les ordinateurs d'extrémité. Les tentatives de désinstallation sont annulées et les tentatives non autorisées sont journalisées.

Si vous utilisez une version de démonstration, assurez-vous que vous paramétrez **Désinstallation autorisée** sur **Oui** avant que la version de démonstration n'expire.

Appliquez la protection antialtération Sophos sur les ordinateurs d'extrémité utilisant Sophos Endpoint Security and Control.

3 À propos de SafeGuard Management Center

SafeGuard Management Center est l'instrument central qui permet d'administrer les ordinateurs chiffrés avec SafeGuard Enterprise. Grâce au SafeGuard Management Center, vous pouvez mettre en place une stratégie de sécurité dans toute l'entreprise et l'appliquer aux ordinateurs d'extrémité. SafeGuard Management Center vous permet de :

- Créer ou importer la structure organisationnelle.
- Créer des responsables de la sécurité.
- Définir des stratégies.
- Exporter et importer des configurations.
- Surveiller les ordinateurs via les fonctionnalités de journalisation étendues.
- Récupérer des mots de passe et l'accès aux ordinateurs chiffrés.

Grâce au SafeGuard Management Center, vous disposer du support mutualisé (Multi Tenancy) pour l'administration de plusieurs domaines et bases de données. Vous pouvez administrer plusieurs bases de données SafeGuard Enterprise et gérer différentes configurations.

Seuls les utilisateurs disposant des privilèges (les responsables de la sécurité) peuvent accéder au SafeGuard Management Center. Plusieurs responsables de la sécurité peuvent travailler simultanément sur les données. Les différents responsables de la sécurité peuvent effectuer leurs opérations conformément aux rôles et aux droits qui leur ont été attribués.

Vous pouvez personnaliser les stratégies et les paramètres selon vos besoins. Après l'enregistrement de nouveaux paramètres dans la base de données, ils peuvent être transférés sur les ordinateurs d'extrémité, où ils deviennent actifs.

Remarque : certaines fonctions ne sont pas incluses dans toutes les licences. Veuillez contacter votre Partenaires commercial pour obtenir plus de renseignements sur ce qui est inclus dans votre licence.

4 Connexion au SafeGuard Management Center

Au cours de la configuration initiale de SafeGuard Enterprise, un compte est créé pour le Responsable principal de la sécurité. Ce compte est obligatoire la première fois que vous vous connectez au SafeGuard Management Center. Pour démarrer le SafeGuard Management Center, l'utilisateur doit connaître le mot de passe du magasin de certificats et disposer de la clé privée du certificat.

Retrouvez plus d'informations dans le *Guide d'installation de SafeGuard Enterprise*.

La procédure de connexion dépend de l'exécution du SafeGuard Management Center connecté à une base de données (mode Single Tenancy) ou à plusieurs bases de données (mode Multi Tenancy).

Remarque : deux responsables de la sécurité ne doivent pas utiliser le même compte Windows sur le même ordinateur. Dans le cas contraire, il est impossible de distinguer correctement leurs droits d'accès.

4.1 Avertissement à l'expiration du certificat d'entreprise

À la connexion, SafeGuard Management Center commence par afficher un avertissement six mois avant l'expiration du certificat d'entreprise et vous invite à le renouveler et à le déployer sur les ordinateurs d'extrémité. Sans certificat d'entreprise valide, un ordinateur d'extrémité ne peut pas se connecter au serveur.

Vous pouvez renouveler le certificat d'entreprise n'importe quand. Même si le certificat d'entreprise a déjà expiré. Un certificat d'entreprise expiré sera aussi indiqué par une boîte de message. Retrouvez plus d'informations sur le renouvellement d'un certificat d'entreprise à la section Renouvellement du certificat d'entreprise à la page 67.

4.2 Connexion en mode Single Tenancy

1. Démarrez SafeGuard Management Center à partir du dossier des produits du menu **Démarrer**. Une boîte de dialogue de connexion apparaît.
2. Connectez-vous en tant que responsable principal de la sécurité (MSO) et saisissez le mot de passe du magasin de certificats spécifié pendant la configuration initiale. Cliquez sur **OK**.

SafeGuard Management Center est ouvert.

Remarque : si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai sera imposé avant la tentative de connexion suivante. Le délai augmente à chaque échec de tentative de connexion. Les tentatives ratées de connexion sont consignées dans le journal.

4.3 Connexion en mode mutualisé (Multi Tenancy)

Le processus de connexion au SafeGuard Management Center est étendu lorsque plusieurs bases de données ont été configurées (Multi Tenancy). Retrouvez plus d'informations à la sectiion Utilisation de plusieurs configurations de bases de données à la page 20.

1. Démarrez SafeGuard Management Center à partir du dossier des produits dans le menu **Démarrer**. La boîte de dialogue **Sélection d'une configuration** s'affiche.
2. Sélectionnez la configuration de base de données que vous souhaitez utiliser dans la liste déroulante et cliquez sur **OK**.

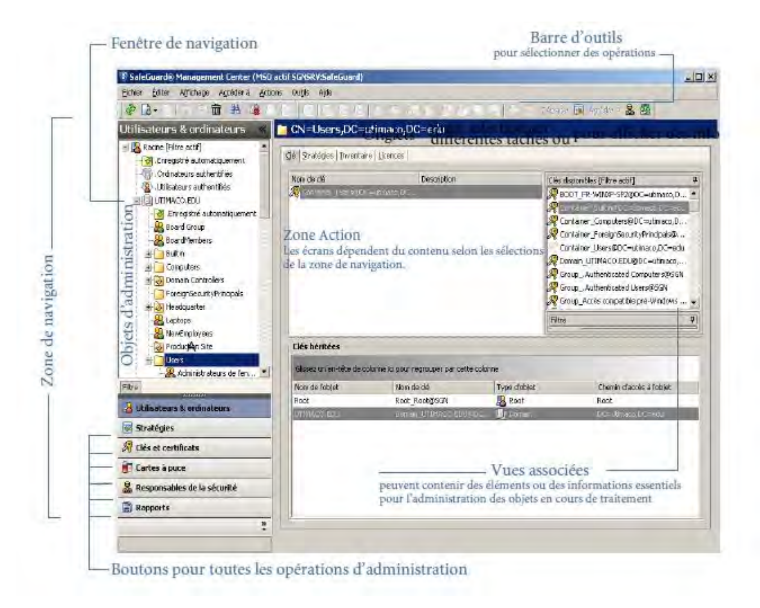
   La configuration de base de données sélectionnée est reliée au SafeGuard Management Center et devient active.

3. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

SafeGuard Management Center est ouvert et relié à la configuration de base de données sélectionnée.

Remarque : si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai augmente à chaque échec de tentative de connexion. Les tentatives ratées de connexion sont consignées dans le journal.

4.4 Interface utilisateur du SafeGuard Management Center



Zone de navigation

La zone de navigation contient des boutons pour toutes les opérations d'administration :

- **Utilisateurs et ordinateurs**

  Pour importer des groupes et des utilisateurs à partir d'un annuaire actif, à partir du domaine ou d'un ordinateur individuel.

- **Stratégies**

  Pour créer des stratégies.

- **Clés et certificats**

  Pour gérer les clés et les certificats.

- **Tokens**

  Pour gérer les tokens et les cartes à puce.

- **Responsables de la sécurité**

  Pour créer des responsables de la sécurité ou des rôles et définir les opérations qui nécessitent une autorisation supplémentaire.

- **Rapports**

  Pour créer et gérer des comptes-rendus de tous les événements liés à la sécurité.

Fenêtre de navigation

Les objets devant être traités ou pouvant être créés apparaissent dans la fenêtre de navigation (objets Active Directory tels que les OU, utilisateurs et ordinateurs, éléments de stratégies, etc.). Les objets affichés dépendent de la tâche sélectionnée.

Remarque : dans **Utilisateurs et ordinateurs**, les objets affichés dans l'arborescence de la fenêtre de navigation dépendent des droits d'accès du responsable de la sécurité pour les objets du répertoire. L'arborescence affiche seulement les objets auxquels peut accéder le responsable de la sécurité connecté. Les objets refusés n'apparaissent pas, sauf s'il existe des nœuds inférieurs dans l'arborescence pour lesquels le responsable de la sécurité a les droits d'accès. Dans ce cas, les objets refusés sont grisés. Si le responsable de la sécurité à les droits d'**Accès complet**, l'objet apparaît en noir. Les objets avec un accès en **Lecture seule** apparaissent en bleu.

Zone d'action

Dans la zone d'action, définissez les paramètres des objets sélectionnés dans la fenêtre de navigation. La zone d'action contient différents onglets permettant de traiter les objets et de définir les paramètres.

La zone d'action comporte également des informations concernant les objets sélectionnés.

Vues associées

Dans ces vues, des objets et des informations supplémentaires apparaissent. Elles fournissent des informations utiles concernant l'administration du système et en simplifient l'utilisation. Vous pouvez par exemple attribuer des clés à des objets avec l'opération de glisser-déplacer.

Barre d'outils

Contient des symboles pour les différentes opérations du SafeGuard Management Center. Les symboles sont affichés tels qu'ils sont disponibles et quand ils sont disponibles pour l'objet sélectionné.

Après la connexion, SafeGuard Management Center s'ouvre toujours avec la vue qui était utilisée lors de sa fermeture.

4.5 Paramètres de langue

Les paramètres de langue pour SafeGuard Management Center et le logiciel de chiffrement SafeGuard Enterprise sur les ordinateurs d'extrémité sont les suivants :

Langue du SafeGuard Management Center

Vous pouvez définir la langue du SafeGuard Management Center ainsi :

- Dans la barre de menus de SafeGuard Management Center, cliquez sur **Outils** > **Options** > **Général**. Sélectionnez **Utiliser la langue définie par l'utilisateur** et sélectionnez une langue disponible. Les langues prises en charge sont l'anglais, l'allemand, le français et le japonais.
- Redémarrez SafeGuard Management Center. Il apparaît dans la langue sélectionnée.

Langue de SafeGuard Enterprise sur les ordinateurs d'extrémité

Vous définissez la langue de SafeGuard Enterprise sur l'ordinateur d'extrémité dans une stratégie de type **Paramètres généraux** dans SafeGuard Management Center en utilisant le paramètre **Personnalisation** > **Langue utilisée sur le client** :

- Si la langue du système d'exploitation est sélectionnée, SafeGuard Enterprise utilise le paramètre de langue du système d'exploitation. Si la langue du système d'exploitation n'est pas disponible dans SafeGuard Enterprise, la langue de SafeGuard Enterprise est définie par défaut sur l'anglais.
- Si l'une des langues disponibles est sélectionnée, les fonctions de SafeGuard Enterprise apparaissent dans la langue sélectionnée sur l'ordinateur d'extrémité.

5 Licences

Vous avez besoin d'une licence valide pour utiliser SafeGuard Enterprise avec le SafeGuard Management Center comme système direct. Par exemple, dans la base de données SafeGuard Enterprise, une licence valide est une condition préalable à l'envoi de stratégies aux ordinateurs d'extrémité. Les licences de token appropriées sont également requises pour la gestion des tokens.

Les fichiers de licence sont disponibles auprès de votre partenaire des ventes. Ces fichiers doivent être importés dans la base de données SafeGuard Enterprise après l'installation.

Le fichier de licence inclut entre autres informations :

- Le nombre de licences achetées par module.
- Le nom du détenteur de la licence.
- Une limite de tolérance spécifiée pour le dépassement du nombre de licences.

Si le nombre de licences disponibles ou la limite de tolérance est dépassé, des messages d'avertissement/erreur correspondants s'affichent au démarrage de SafeGuard Management Center.

Dans la zone **Utilisateurs et ordinateurs**, SafeGuard Management Center propose un aperçu de l'état de la licence du système SafeGuard Enterprise installé. L'affichage de l'état de la licence est disponible dans l'onglet **Licences** du nœud racine, des domaines, des OU, des objets conteneurs et des groupes de travail. C'est là que les responsables de la sécurité peuvent trouver des informations détaillées sur l'état de la licence. S'ils ont les droits suffisants, ils peuvent importer des licences dans la base de données SafeGuard Enterprise.

5.1 Fichier de licence

Le fichier de licence que vous recevez pour être importé dans la base de données SafeGuard Enterprise est un fichier .XML avec une signature. Le fichier de licence inclut les informations suivantes :

- Nom de la société
- Informations supplémentaires (département, filiale par exemple)
- Date de génération
- Nombre de licences par module
- Informations sur la licence du token
- Date d'expiration de la licence
- Type de licence (démonstration ou complète)
- Signature avec le certificat de signature de licence

5.2 Licences de token

Pour gérer des tokens ou des cartes à puce, les licences de token appropriées sont requises. Si les licences appropriées ne sont pas disponibles, vous ne pouvez pas créer de stratégies pour les tokens dans SafeGuard Management Center.

5.3 Licences d'évaluation et de démonstration

Le fichier de licence par défaut (licence d'évaluation) ou les fichiers de licence de démonstration individuels peuvent être utilisés pour l'évaluation ou le déploiement initial. Ces licences sont uniquement valides pendant une certaine période de temps et ont une date d'expiration. En revanche il n'existe aucune restriction fonctionnelle.

Remarque : les licences d'évaluation et de démonstration ne doivent pas être utilisées dans un environnement de travail normal.

5.3.1 Fichiers de licence par défaut

Un fichier de licence par défaut est chargé automatiquement lors de l'installation du SafeGuard Management Center. Cette licence d'évaluation (appelée licence d'évaluation de SafeGuard Enterprise) contient cinq licences pour chaque module et est limitée pour une durée de deux ans à compter de la date de publication de la version SafeGuard Enterprise en question.

Fichier de licence par défaut pour SafeGuard Cloud Storage et pour SafeGuard File Encryption

Lorsque SafeGuard Management Center 6.1 est installé, un fichier de licence par défaut supplémentaire est chargé automatiquement pour SafeGuard Cloud Storage et pour SafeGuard File Encryption. Cette licence d'évaluation contient cinq licences pour chacun des deux modules et elle est valable pendant deux ans à compter de la date de sortie de SafeGuard Enterprise 6.1.

Remarque : lors de la mise à niveau de SafeGuard Enterprise 5.x à SafeGuard Enterprise 6.1, vous devez importer manuellement ce fichier de licence dans la base de données de SafeGuard Enterprise.

5.3.2 Fichiers de licence de démonstration individuelle

Si le fichier de licence par défaut ne suffit pas à l'évaluation, vous pouvez également obtenir une licence de démonstration personnalisée en fonction de vos besoins. Pour obtenir un fichier de licence de démonstration individuelle, veuillez contacter votre partenaire de ventes. Ce type de démonstration de licence est également limité dans le temps. La licence est également limitée au nombre de licences par module accordé par votre partenaire commercial.

Lorsque vous démarrez SafeGuard Management Center, un message d'avertissement indique que vous utilisez des licences de démonstration. Si le nombre de licences disponibles indiqué dans la licence de démonstration est dépassé ou si la durée limite est atteinte, un message d'erreur s'affiche.

5.4 Aperçu de l'état de la licence

Pour afficher un aperçu de l'état de la licence :

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation à gauche, cliquez sur le nœud racine, le domaine, l'OU, l'objet conteneur ou le groupe de travail.
3. Dans la zone d'action, accédez à l'onglet **Licences** à droite.

L'état de la licence apparaît.

L'écran est divisé en trois zones. La zone supérieure indique le nom du client pour lequel la licence a été générée ainsi que la date de génération.

La zone centrale propose des détails sur la licence. Les colonnes individuelles contiennent les informations suivantes :

Colonne	Explication
État (icône)	Une icône indique le statut de la licence (validité, message d'avertissement, message d'erreur) du module concerné.
Fonction	Indique le module installé.
Licences achetées	Indique le nombre de licences achetées pour le module installé.
Licences utilisées	Indique le nombre de licences utilisées pour le module installé.
Expire	Indique la date d'expiration de la licence.
Type	Indique le type de licence, démonstration ou standard.
Limite de tolérance	Indique la limite de tolérance spécifiée pour le dépassement du nombre de licences achetées.

Si vous affichez l'onglet **Licences** d'un domaine/OU, l'aperçu indique le statut en fonction de l'ordinateur de la branche concernée.

Des détails sur les modules de token sous licence sont proposés sous cette présentation.

Dans la partie inférieure, un message avec une couleur d'arrière-plan spécifique à l'état (vert = valide, jaune = avertissement, rouge = erreur) et une icône indiquent le statut global de la licence, quel que soit le domaine ou l'OU sélectionné. Si cette partie indique un message d'avertissement ou d'erreur, il affiche aussi des informations sur la restauration d'un état de licence valide.

Les icônes affichées dans l'onglet **Licences** ont les significations suivantes :

	Licence valide
	Avertissement La licence d'un module affiche un état d'avertissement si ■ La limite de la licence est dépassée. ■ La licence a expiré.
	Erreur La licence d'un module affiche un état d'erreur si ■ La seuil de tolérance est dépassé. ■ La licence a expiré il y a plus d'un mois.

Pour actualiser l'aperçu de l'état de la licence, cliquez sur **Recompter les licences utilisées**.

5.5 Importation de fichiers de licence

Condition préalable : pour importer un fichier de licence dans la base de données SafeGuard Enterprise, un responsable de la sécurité doit disposer du droit "Importer le fichier de licence".

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation, à gauche, cliquez sur le nœud racine, le domaine ou l'unité organisationnelle.
3. Dans la zone d'action, changez pour l'onglet **Licences**.
4. Cliquez sur le bouton **Importer le fichier de licence...**.

   Une fenêtre s'ouvre dans laquelle vous pouvez sélectionner le fichier de licence.

5. Sélectionnez le fichier de licence que vous souhaitez importer, puis cliquez sur **Ouvrir**.

   La boîte de dialogue **Application de la licence ?** apparaît avec le contenu du fichier de licence.

6. Cliquez sur **Appliquer la licence**.

Le fichier de licence est importé dans la base de données SafeGuard Enterprise.

Après avoir importé le fichier de licence, les licences de module achetées sont indiquées par le type de licence **standard**. Tous les modules pour lesquels aucune licence n'a été achetée et pour lequel la licence d'évaluation (fichier de licence par défaut) ou des licences de démonstration individuelles sont utilisées sont marqués avec le type de licence **démonstration**.

Remarque : lorsqu'un nouveau fichier de licence est importé, seuls les modules inclus dans ce fichier de licence sont affectés. Toute autre information de licence de module est conservée telle que récupérée depuis la base de données. Ces fonctionnalités d'importation simplifient l'évaluation des modules supplémentaires après que vous en avez acheté un ou plusieurs modules.

5.6 Licence dépassée

Une valeur de tolérance a été définie dans votre fichier de licence quant au dépassement du nombre de licences achetées et à la période de validité de la licence. Si le nombre de licences disponibles par module ou la période de validité est dépassé, un message d'avertissement s'affiche. Ceci n'affecte pas l'utilisation du système et aucune restriction n'affecte ses fonctionnalités. Vous pouvez réviser l'état de la licence et mettre à niveau ou renouveler votre licence. La valeur de tolérance est généralement de 10 % du nombre de licences achetées (la valeur minimale est 5, la valeur maximale est 5 000).

Un message d'erreur s'affiche si la valeur de tolérance est dépassée. Dans ce cas, les fonctionnalités sont restreintes. Le déploiement des stratégies sur les ordinateurs d'extrémité est désactivé. Cette désactivation ne peut pas être inversée manuellement dans SafeGuard Management Center. La licence doit être mise à niveau ou renouvelée pour pouvoir de nouveau bénéficier de toutes les fonctions. Outre la désactivation du déploiement des stratégies, la restriction fonctionnelle n'affecte pas les ordinateurs d'extrémité. Les stratégies affectées restent actives. Les clients peuvent également être désinstallés.

Les sections suivantes décrivent le comportement du système en cas de dépassement du nombre de licences autorisées ainsi que l'action nécessaire pour restaurer la restriction fonctionnelle.

5.6.1 Licence non valide : avertissement

Si le nombre de licences disponibles est dépassé, un avertissement apparaît au démarrage du SafeGuard Management Center.

SafeGuard Management Center s'ouvre et affiche la présentation de l'état de la licence dans la zone **Utilisateurs et ordinateurs** de l'onglet **Licences**.

Un message d'avertissement vous informe que la licence n'est pas valide. À l'aide des informations détaillées sur le fichier de licence, vous pouvez déterminer le module pour lequel le nombre de licences disponibles est dépassé. Cet état de la licence peut être modifié en faisant évoluer, en renouvelant ou en mettant la licence à niveau.

5.6.2 Licence non valide : erreur

Si la valeur de tolérance du nombre de licences ou la période de validité définie dans la licence est dépassée, SafeGuard Management Center affiche un message d'erreur.

Dans SafeGuard Management Center, le déploiement de stratégies sur les ordinateurs d'extrémité est désactivé.

Un message d'erreur s'affiche dans la zone **Utilisateurs et ordinateurs** de l'onglet **Licences**.

À l'aide des informations détaillées sur le fichier de licence, vous pouvez déterminer le module pour lequel le nombre de licences disponibles est dépassé.

Pour surmonter la restriction de fonctionnalité, vous pouvez :

- Redistribuer des licences

  Pour mettre à disposition les licences, vous pouvez désinstaller le logiciel sur les ordinateurs d'extrémité non utilisés et supprimer ainsi les ordinateurs de la base de données SafeGuard Enterprise.

- Mettre à niveau/renouveler des licences

  Contactez votre partenaire commercial pour mettre à niveau ou renouveler votre licence. Vous recevrez un nouveau fichier de licence à importer dans la base de données SafeGuard Enterprise.

- Importer un nouveau fichier de licence

  Si vous avez renouvelé ou mis à niveau votre licence, vous pouvez importer le fichier de licence dans la base de données SafeGuard Enterprise. Ce nouveau fichier importé remplace le fichier de licence non valide.

Dès que vous redistribuez des licences ou que vous importez un fichier de licence valide, la restriction fonctionnelle est annulée et le système fonctionne à nouveau normalement.

6 Utilisation de plusieurs configurations de base de données

SafeGuard Management Center permet d'utiliser plusieurs configurations de base de données (mode Multi-Tenancy ou plusieurs titulaires). Pour utiliser cette fonction, vous devez l'activer pendant l'installation. Retrouvez plus d'informations dans le *Guide d'installation de SafeGuard Enterprise*.

Le mode Multi Tenancy vous permet de configurer différentes configurations de base de données SafeGuard Enterprise et de les gérer pour une instance du SafeGuard Management Center. Ceci est tout particulièrement utile si vous souhaitez disposer de configurations différentes pour des domaines, des unités organisationnelles ou des lieux différents.

Condition préalable : la fonction de configuration Multi Tenancy doit avoir été installée via une installation de type **Complète**. La configuration initiale du SafeGuard Management Center doit avoir été réalisée.

Pour simplifier la configuration, vous pouvez :

- créer plusieurs configurations de base de données ;
- sélectionner des configurations de base de données créées précédemment ;
- supprimer des configurations de base de données de la liste ;
- importer une configuration de base de données créée précédemment à partir d'un fichier ;
- exporter une configuration de base de données à réutiliser ultérieurement.

6.1 Création de configurations de base de données supplémentaires

Pour créer une configuration de base de données supplémentaire SafeGuard Enterprise à la suite de la configuration initiale :

1. Démarrez le SafeGuard Management Center.

   La boîte de dialogue **Sélection d'une configuration** s'affiche.

2. Cliquez sur **Nouveau**.

   L'assistant de configuration de SafeGuard Management Center démarre automatiquement L'assistant vous guide tout au long des étapes nécessaires de création d'une nouvelle configuration de base de données.

3. Spécifiez les paramètres selon vos besoins.

   La nouvelle configuration de base de données est créée.

4. Pour vous authentifier dans le SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

SafeGuard Management Center est ouvert et relié à la nouvelle configuration de base de données. Au prochain lancement du SafeGuard Management Center, la nouvelle configuration de base de données peut être sélectionnée dans la liste.

6.2 Association à une configuration de base de données existante

Pour travailler avec une configuration de base de données SafeGuard Enterprise :

1. Démarrez le SafeGuard Management Center.

   La boîte de dialogue **Sélection d'une configuration** s'affiche.

2. Sélectionnez la configuration de base de données souhaitée dans la liste déroulante et cliquez sur **OK**.

   La configuration de base de données sélectionnée est reliée au SafeGuard Management Center et devient active.

3. Pour vous authentifier dans le SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

Le SafeGuard Management Center démarre et se connecte à la configuration de base de données sélectionnée.

6.3 Exportation d'une configuration dans un fichier

Pour enregistrer ou réutiliser une configuration de base de données, vous pouvez l'exporter dans un fichier :

1. Démarrez le SafeGuard Management Center.

   La boîte de dialogue **Sélection d'une configuration** s'affiche.

2. Sélectionnez la configuration de base de données respective dans la liste et cliquez sur **Exporter...**.
3. Pour sécuriser le fichier de configuration, vous êtes invité à saisir et à confirmer un mot de passe qui chiffre le fichier de configuration. Cliquez sur **OK**.
4. Spécifiez un nom et un emplacement de stockage pour le fichier de configuration exporté *.SGNConfig.

   Si cette configuration existe déjà, vous êtes invité à confirmer le remplacement de la configuration existante.

Le fichier de configuration de base de données est enregistré à l'emplacement de stockage spécifié.

6.4 Importation d'une configuration à partir d'un fichier

Pour utiliser ou modifier une configuration de base de données, vous pouvez importer une configuration créée précédemment dans SafeGuard Management Center. Pour ce faire, vous pouvez procéder de deux façons :

- via le SafeGuard Management Center (Multi Tenancy)
- en cliquant deux fois sur le fichier de configuration (Single et Multi Tenancy).

6.5 Importation d'une configuration avec SafeGuard Management Center

1. Démarrez SafeGuard Management Center.

   La boîte de dialogue **Sélection d'une configuration** s'affiche.

2. Cliquez sur **Importer...**, recherchez le fichier de configuration souhaité, puis cliquez sur **Ouvrir**.
3. Entrez le mot de passe du fichier de configuration défini lors de l'exportation, puis cliquez sur **OK**.

   La configuration sélectionnée s'affiche.

4. Pour activer la configuration, cliquez sur **OK**.
5. Pour vous authentifier dans le SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

SafeGuard Management Center est ouvert et relié à la configuration de base de données importée.

6.6 Importation d'une configuration en cliquant deux fois sur le fichier de configuration (Single et Multi Tenancy)

Remarque : cette tâche est disponible en mode Single Tenancy et Multi Tenancy.

Vous pouvez également exporter une configuration et la distribuer vers plusieurs responsables de la sécurité. Les responsables de la sécurité cliquent deux fois alors sur le fichier de configuration pour ouvrir une instance du SafeGuard Management Center totalement configurée.

Ceci est utile lorsque vous utilisez l'authentification SQL pour la base de données et souhaitez éviter que chaque administrateur connaisse le mot de passe SQL. Dans ce cas, vous ne le saisissez ensuite qu'une seule fois, vous créez un fichier de configuration et vous le distribuez vers les ordinateurs des responsables de la sécurité concernés.

Condition préalable : la configuration initiale du SafeGuard Management Center doit avoir été effectuée. Retrouvez plus d'informations dans le *Guide d'installation de SafeGuard Enterprise*.

1. Démarrez SafeGuard Management Center.

2. Sélectionnez **Options** dans le menu **Outils** et sélectionnez l'onglet **Base de données**.
3. Saisissez et confirmez les codes d'accès de la connexion au serveur de base de données SQL.
4. Cliquez sur **Exporter la configuration** pour exporter cette configuration vers un fichier.
5. Saisissez et confirmez un mot de passe pour le fichier de configuration.
6. Saisissez un nom de fichier et spécifiez un emplacement de stockage.
7. Déployez ce fichier de configuration sur les ordinateurs des responsables de la sécurité. Fournissez-leur le mot de passe de ce fichier et du magasin de certificats nécessaires pour s'authentifier dans SafeGuard Management Center.
8. Les responsables de la sécurité cliquent simplement deux fois sur le fichier de configuration.
9. Ils sont invités à saisir le mot de passe du fichier de configuration.
10. Pour s'authentifier sur SafeGuard Management Center, ils sont invités à saisir leur mot de passe de magasin de certificats.

SafeGuard Management Center démarre avec la configuration importée. Cette configuration est la nouvelle configuration par défaut.

6.7 Basculement rapide entre les configurations de base de données

Pour simplifier la gestion de plusieurs titulaires, le SafeGuard Management Center permet de basculer rapidement entre les configurations de base de données.

Remarque : cette tâche est également disponible en mode Single Tenancy.

1. Dans le SafeGuard Management Center, sélectionnez **Changer la configuration...** dans le menu **Fichier**.
2. Dans la liste déroulante, sélectionnez la base de données à laquelle vous souhaitez basculer et cliquez sur **OK**.

SafeGuard Management Center redémarre automatiquement avec la configuration sélectionnée.

6.8 Vérification de l'intégrité de la base de données

Lorsque vous vous connectez à la base de données, l'intégrité de cette dernière est vérifiée automatiquement. La boîte de dialogue **Vérifier l'intégrité de la base de données** s'affiche si cette vérification renvoie des erreurs.

Vous pouvez également lancer la vérification de l'intégrité de la base de données et afficher la boîte de dialogue **Vérifier l'intégrité de la base de données** :

1. Dans le SafeGuard Management Center, sélectionnez **Outils** > **Intégrité de la base de données** dans la barre de menus.
2. Vérifiez les tables en cliquant sur **Tout vérifier** ou **Vérifier la sélection**.

Les tables erronées sont indiquées dans la boîte de dialogue. Pour les réparer, cliquez sur **Réparer**.

Remarque : suite à la sauvegarde d'une mise à jour SafeGuard Enterprise (SQL), la vérification de l'intégrité de la base de données sera toujours déclenchée en premier. Les vérifications

doivent uniquement être effectuées une seule fois par base de données SafeGuard Enterprise afin d'effectuer la mise à jour.

7 Création de la structure organisationnelle

La structure organisationnelle peut se refléter dans le SafeGuard Management Center de deux façons :

- Vous pouvez importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise, par exemple par l'intermédiaire d'un Active Directory.
- Vous pouvez créer manuellement votre structure organisationnelle en créant des groupes de travail et des domaines ainsi qu'une structure pour la gestion des éléments de la stratégie.

7.1 Importation depuis Active Directory

Vous pouvez importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise, par exemple par l'intermédiaire d'un Active Directory.

Nous vous recommandons de créer un compte de service Windows dédié qui sera utilisé pour toutes les tâches d'importation et de synchronisation, ceci pour garantir une importation correcte et pour empêcher la suppression accidentelle d'objets dans la base de données SafeGuard Enterprise. Retrouvez plus d'informations sur l'attribution des droits dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/107979.aspx.

7.1.1 Importation de la structure organisationnelle

Remarque : avec le Planificateur de tâches SafeGuard Management, vous pouvez créer des tâches périodiques pour la synchronisation automatique entre Active Directory et SafeGuard Enterprise. Votre produit livré contient à cet effet un modèle de script prédéfini. Retrouvez plus d'informations à la section Planification des tâches à la page 267 et à la section Scripts prédéfinis pour les tâches périodiques à la page 273.

1. Dans SafeGuard Management Center, sélectionnez **Outils** > **Options.**
2. Sélectionnez l'onglet **Répertoire** et cliquez sur **Ajouter**.
3. Dans **Authentification LDAP**, procédez comme suit :

   a) Dans le champ **Nom ou adresse IP du serveur**, saisissez le nom NetBIOS du contrôleur de domaine ou son adresse IP.

   b) Pour **Codes d'accès de l'utilisateur**, saisissez votre nom et votre mot de passe Windows pour vous connecter à l'environnement (test).

   c) Cliquez sur **OK**.

   Remarque : pour les ordinateurs autonomes Windows, un répertoire doit être partagé pour activer une connexion via LDAP.

4. Cliquez sur **Utilisateurs et ordinateurs**.
5. Dans la fenêtre de navigation de gauche, cliquez sur le répertoire racine **Racine** [**Filtre actif**].
6. Dans la zone d'action de droite, sélectionnez l'onglet **Synchroniser**.

7. Sélectionnez le répertoire requis dans la liste **DSN répertoire** et cliquez sur l'icône de la loupe (en haut à droite).

   Une représentation graphique de la structure Active Directory des unités organisationnelles de votre entreprise s'affiche.

8. Cochez les unités organisationnelles (OU) qui doivent être synchronisées. Il n'est pas nécessaire d'importer l'ensemble du contenu d'Active Directory.
9. Pour également synchroniser les appartenances, sélectionnez la case à cocher **Synchroniser l'appartenance**. Pour également synchroniser l'état activé par l'utilisateur, sélectionnez la case à cocher **Synchroniser l'état activé par l'utilisateur**.
10. Au bas de la zone d'action, cliquez sur **Synchroniser**.

    Lors de la synchronisation d'utilisateurs avec leur appartenance à un groupe, l'appartenance à un "groupe principal" n'est pas synchronisée car elle n'est pas visible pour le groupe.

Les domaines sont synchronisés. Des informations sur la synchronisation s'affichent. Cliquez sur le message qui s'affichent dans la barre d'état en dessous à gauche des boutons pour voir un protocole de synchronisation. Cliquez sur le protocole, pour le copier dans le Presse-papiers et le coller dans un e-mail ou un fichier.

Remarque : si des éléments ont été déplacés d'une sous-arborescence vers une autre dans Active Directory, les deux sous-arborescences doivent être synchronisées avec la base de données SQL. La synchronisation d'une seule sous-arborescence aboutit à la suppression d'objets au lieu de leur déplacement.

Remarque : nous vous recommandons de diviser en plusieurs opérations l'importation de plus de 400 000 objets depuis AD. Il se peut que l'opération ne soit pas possible s'il y a plus de 400 000 objets dans une seule unité organisationnelle.

7.1.2 Importation d'un nouveau domaine à partir d'un Active Directory

1. Dans la fenêtre de navigation de gauche, cliquez sur le répertoire racine **Racine** [**Filtre actif**].
2. Sélectionnez **Fichier** > **Nouveau Importer nouveau domaine de AD**.
3. Dans la zone d'action de droite, sélectionnez **Synchroniser**.
4. Sélectionnez le répertoire requis dans la liste **DSN répertoire** et cliquez sur l'icône de la loupe (en haut à droite).

   Une représentation graphique de la structure Active Directory des unités organisationnelles de votre entreprise s'affiche.

5. Cochez le domaine à synchroniser et cliquez sur **Synchroniser** au bas de la zone de navigation.

Remarque : si des éléments ont été déplacés d'une sous-arborescence vers une autre dans Active Directory, les deux sous-arborescences doivent être synchronisées avec la base de données SQL. La synchronisation d'une seule sous-arborescence aboutit à la suppression d'objets au lieu de leur déplacement.

Remarque : la synchronisation AD ne synchronise pas le nom avant Windows 2000 (NetBIOS) du domaine, si le contrôleur de domaine est configuré avec une adresse IP. Configurez le

contrôleur de domaine pour utiliser le nom de serveur (NetBIOS ou DNS) à la place. Le client (sur lequel la synchronisation AD fonctionne) doit soit faire partie du domaine, soit pouvoir résoudre le nom DNS vers le contrôleur de domaine cible.

7.1.3 Droits d'accès du responsable de la sécurité et importation Active Directory

La règle suivante s'applique pour importer la structure organisationnelle depuis un Active Directory pour ce qui concerne les droits d'accès requis :

- Pour la gestion des connexion Active Directory, la règle suivante s'applique, si vous ajoutez une connexion Active Directory à un domaine qui existe déjà :
  - Si vous avez les droits d'**Accès complet** pour le domaine (DNS), les codes d'accès de connexion au répertoire sont mises à jour.
  - Si vous avez des droits **Lecture seule** ou moins pour le domaine (DNS), les codes d'accès ne sont pas mis à jour, mais vous pouvez utiliser des codes d'accès existants à des fins de synchronisation.
- Pour l'importation et la synchronisation Active Directory, les droits d'accès à un conteneur ou à un domaine englobent l'arborescence de domaine que vous pouvez importer ou synchroniser. Si vous n'avez pas les droits **Accès complet** pour une arborescence secondaire, il ne peut pas être synchronisé. Si une sous-arborescence ne peut pas être modifiée, elle n'apparaît pas dans l'arborescence de synchronisation.
- Quels que soient les droits d'accès aux objets du répertoire de votre responsable de la sécurité, vous pouvez importer un nouveau domaine depuis l'Active Directory, s'il n'existe pas encore dans la base de données SafeGuard Enterprise. Des droits d'**Accès complet** au nouveau domaine seront accordés automatiquement à vous et à votre responsable de la sécurité.
- Si vous sélectionnez un sous-conteneur pour la synchronisation, celle-ci doit être effectuée jusqu'à la racine. Dans l'arborescence de synchronisation, tous les conteneurs correspondants sont sélectionnés automatiquement, même s'il y a des conteneurs au-dessus du sous-conteneur qui sont en **Lecture seule** ou **Refusés** en fonction de vos droits d'accès. Si vous dessélectionnez un sous-conteneur, vous allez également devoir, en fonction de vos droits d'accès, dessélectionner les conteneurs jusqu'à la racine,.

  Si un groupe avec un accès en **Lecture seule** ou **Refusé** est inclus dans un processus de synchronisation, voici ce qui se passe :

  - Les appartenances du groupe ne sont pas mises à jour.
  - Si le groupe a été supprimé dans l'Active Directory, il ne sera pourtant pas supprimé de la base de données SafeGuard Enterprise.
  - Si, par contre, le groupe a été déplacé dans l'Active Directory, il sera déplacé dans la structure SafeGuard Enterprise, même dans un conteneur pour lequel vous n'avez pas les droits d'**Accès complet**.

  Si un conteneur avec un accès en **Lecture seule** ou **Refusé** est inclus à la synchronisation parce qu'il se trouve à la racine et s'il contient un groupe avec **Accès complet**, ce groupe sera synchronisé. Les groupes avec un accès en **Lecture seule** ou **Refusé** ne le seront pas.

7.2 Création des groupes de travail et des domaines

Les responsables de la sécurité avec les droits nécessaires peuvent créer manuellement des groupes de travail ou des domaines avec une structure de gestion des éléments de la stratégie. Il est également possible d'attribuer des stratégies et/ou des stratégies de chiffrement aux utilisateurs locaux.

Veuillez créer un nouveau domaine uniquement si vous ne voulez pas ou ne pouvez pas importer un domaine à partir d'Active Directory (AD) (par exemple, parce qu'aucun AD n'est disponible).

7.2.1 Enregistrement d'un nouvel utilisateur

Retrouvez plus d'informations sur la première connexion des utilisateurs à SafeGuard Enterprise à la section Authentification au démarrage de SafeGuard à la page 87.

Lorsqu'un nouvel utilisateur se connecte à SafeGuard Enterprise dès que son ordinateur a contacté le serveur SafeGuard Enterprise, il est enregistré et apparaît automatiquement dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center sous son domaine ou groupe de travail respectif.

Le répertoire de ces utilisateurs/ordinateurs (**.Enregistré automatiquement**) est créé automatiquement sous le répertoire racine et sous chaque domaine/groupe de travail. Il ne peut être ni renommé ni déplacé. Les objets de ce répertoire ne peuvent pas non plus être déplacés manuellement. Lorsque l'unité organisationnelle (OU) est synchronisée avec le contact suivant dans la base de données SafeGuard Enterprise, l'objet est déplacé vers l'unité organisationnelle respective. Autrement, il reste sous le répertoire **.Enregistré automatiquement** de son domaine/groupe de travail.

En tant que responsable de la sécurité, vous pouvez alors gérer les objets enregistrés automatiquement comme vous le faites habituellement.

Remarque : les utilisateurs locaux ne peuvent pas se connecter à SafeGuard Enterprise avec un mot de passe vide. Les utilisateurs locaux qui se connectent à SafeGuard Enterprise avec un mot de passe vide restent des invités et ne sont pas enregistrés dans la base de données. Si l'ouverture de session automatique Windows est activée pour ces utilisateurs, la connexion est refusée. Pour se connecter à SafeGuard Enterprise, un nouveau mot de passe doit être créé et l'ouverture de session automatique Windows doit être désactivée dans le registre de l'ordinateur d'extrémité.

Remarque : les comptes Microsoft sont toujours considérés comme des utilisateurs invités de SafeGuard Enterprise.

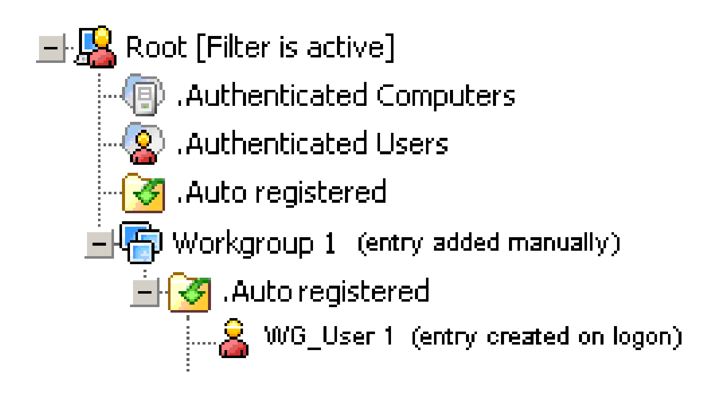
7.2.2 Exemples d'enregistrement automatique

Vous trouverez ci-après deux exemples de comportement d'objets enregistrés automatiquement.

Utilisateurs/ordinateurs ne faisant pas partie d'un Active Directory

Dans une entreprise, tous les objets utilisateur ou ordinateur ne font pas nécessairement partie d'un Active Directory (AD), les utilisateurs locaux par exemple. Une entreprise peut disposer d'un ou de plusieurs groupes de travail, un AD n'est donc pas nécessaire.

Cette entreprise souhaite déployer SafeGuard Enterprise, puis ajouter des stratégies à ses objets utilisateur/ordinateur. La structure organisationnelle de l'entreprise doit donc être créée manuellement dans le SafeGuard Management Center comme suit :



Les objets restent dans le dossier .Auto registered. Ils peuvent être gérés correctement à l'aide de SafeGuard Management Center en appliquant des stratégies sur le dossier .Auto registered.

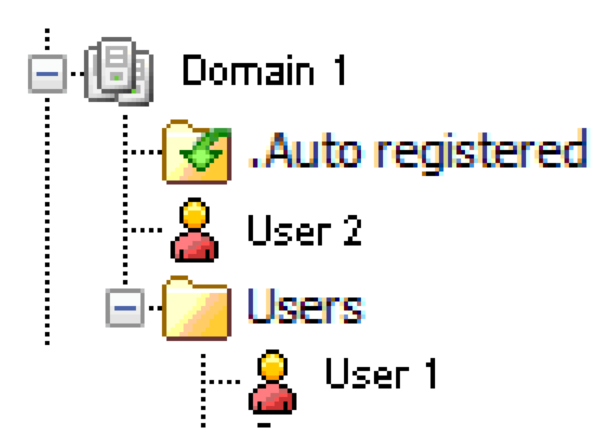
Base de données de SafeGuard Enterprise et Active Directory non synchronisés

Un utilisateur fait déjà partie de l'Active Directory (AD) de l'entreprise. La base de données de SafeGuard Enterprise et l'AD ne sont cependant pas synchronisés. L'utilisateur (**Utilisateur 1**) se connecte à SafeGuard Enterprise et il apparaît automatiquement dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center sous le domaine fourni avec la connexion (**Domaine 1**).



L'utilisateur fait désormais partie du dossier .Auto registered. L'objet peut être géré correctement à l'aide de SafeGuard Management Center en appliquant des stratégies sur le dossier .Auto registered.

À la prochaine synchronisation entre l'AD et la base de données SafeGuard Enterprise, **Utilisateur 1** sera automatiquement déplacé dans son unité organisationnelle (**Utilisateurs**).



Pour activer les stratégies pour l'**Utilisateur 1**, celles-ci doivent désormais être attribuées à l'unité organisationnelle **Utilisateurs**.

7.2.3 Clés et certificats pour les objets enregistrés automatiquement

Pour chaque objet enregistré automatiquement, un certificat est généré en fonction des besoins par le serveur.

Un utilisateur local obtient deux clés:

- la clé du conteneur .Auto registered
- la clé privée générée en fonction des besoins par le serveur

Les utilisateurs locaux n'obtiennent aucune autre clé pour leur conteneur attribué ni de clé racine.

Les groupes de travail n'obtiennent pas de clé.

7.2.4 Stratégies pour les objets enregistrés automatiquement

Pour les objets enregistrés automatiquement, les stratégies peuvent être créées sans aucune restriction.

Les utilisateurs locaux sont ajoutés au groupe "Utilisateurs authentifiés". Les ordinateurs sont ajoutés au groupe "Ordinateurs authentifiés". Les stratégies activées pour ces groupes s'appliquent en conséquence.

7.2.5 Création de groupes de travail

Les responsables de la sécurité disposant des droits requis peuvent créer un conteneur sous le répertoire racine qui représente un groupe de travail Windows. Les groupes de travail n'ont pas de clé. Ils ne peuvent pas être renommés.

1. Dans le SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.

2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur **Racine** [**Filtre actif**] et sélectionnez **Nouveau** > **Créer un nouveau groupe de travail** (**enregistrement auto**).
3. Sous **Informations communes**, indiquez les éléments suivants :
   a) Saisissez un **Nom complet** pour le groupe de travail.
   b) Vous pouvez éventuellement ajouter une **description**.
   c) Le type d'objet est affiché dans le champ **État de connexion**, dans ce cas **Groupe de travail**.
   d) Pour empêcher l'héritage de stratégie, vous pouvez sélectionner **Bloquer l'héritage de stratégie**.
   e) Cliquez sur **OK**.

Le groupe de travail est créé. Le répertoire **.Enregistré automatiquement** par défaut est créé automatiquement sous le conteneur du groupe de travail. Il ne peut être ni renommé ni supprimé.

7.2.6 Suppression de groupes de travail

Pour supprimer des groupes de travail, vous avez besoin des droits d'**Accès complet** pour le groupe de travail concerné. Les membres appartenant au groupe de travail sont également supprimés. Ils sont réenregistrés automatiquement lors de la prochaine connexion.

Pour supprimer un groupe de travail, vous avez besoin des droits d'**Accès complet** pour tous les objets concernés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur le groupe de travail que vous voulez supprimer et sélectionnez **Supprimer**.
3. Pour confirmer, cliquez sur **Oui**.

Le groupe de travail est supprimé. Ses membres éventuels sont également supprimés.

Remarque : si vous n'avez pas les droits d'**Accès complet** pour tous les membres du groupe de travail, la suppression du groupe de travail échoue et un message d'erreur apparaît.

7.2.7 Création d'un domaine

Les responsables de la sécurité disposant des droits requis peuvent créer un domaine sous le répertoire racine. Veuillez créer un nouveau domaine uniquement si vous ne voulez pas ou ne pouvez pas importer un domaine à partir d'Active Directory (AD) (par exemple, parce qu'aucun AD n'est disponible).

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur **Racine** [**Filtre actif**] et sélectionnez **Nouveau** > **Créer un domaine** (**enregistrement auto**).
3. Sous **Informations communes**, saisissez les informations suivantes concernant le contrôleur de domaine.

Les trois entrées de noms doivent être correctes. Faute de quoi le domaine n'est pas synchronisé.

a) **Nom complet :** par exemple *nom ordinateur.domaine.fr* ou l'adresse IP du contrôleur de domaine

b) **Nom distinctif** : nom DNS, par exemple **`DC=nomordinateur3,DC=domaine,DC=pays`**

c) Une description de domaine (facultatif)

d) **Nom Netbios** : nom du contrôleur de domaine

e) Le type d'objet est affiché sous **État de la connexion**, dans ce cas **Domaine**.

f) Pour empêcher l'héritage de stratégie, vous pouvez sélectionner **Bloquer l'héritage de stratégie**.

g) Cliquez sur **OK**.

Le nouveau domaine est créé. Les utilisateurs et/ou ordinateurs sont automatiquement attribués à ce domaine au cours de l'enregistrement automatique. Le répertoire par défaut **.Enregistré automatiquement** est créé automatiquement sous le conteneur du domaine. Il ne peut être ni renommé ni supprimé.

7.2.8 Changement de nom d'un domaine

Les responsables de la sécurité disposant des droits requis peuvent renommer un domaine et définir des propriétés supplémentaires. Vous avez besoin des droits d'**Accès complet** pour le domaine correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur le domaine à renommer puis sélectionnez **Propriétés**.
3. Dans **Informations communes**, sous **Nom complet**, changez le nom du domaine et sa description.
4. Vous pouvez changer le nom du contrôleur de domaine dans **Nom NetBios**.
5. Vous pouvez également définir le mode Éveil par appel réseau pour le redémarrage automatique dans l'onglet **Paramètres de conteneur**.
6. Pour confirmer, cliquez sur **OK**.

À présent, les modifications sont enregistrées.

7.2.9 Suppression d'un domaine

Les responsables de la sécurité dotés des droits requis peuvent supprimer des domaines. Pour supprimer un domaine, vous avez besoin des droits d'**Accès complet** pour le domaine concerné.

Remarque : les membres appartenant au domaine sont également supprimés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.

2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit sur le domaine à supprimer puis sélectionnez **Supprimer**.
3. Cliquez sur **Oui**.

Le domaine est supprimé. Ses membres éventuels sont également supprimés.

Remarque : si vous avez moins que les droits d'**Accès complet** pour tous les membres du domaine, la suppression du domaine échoue et un message d'erreur apparaît.

7.2.10 Suppression des ordinateurs enregistrés automatiquement

Lorsqu'un ordinateur enregistré automatiquement est supprimé, tous les utilisateurs locaux de cet ordinateur le sont également. Ils sont réenregistrés automatiquement lors de leur prochaine connexion à cet ordinateur.

7.2.11 Filtre pour les objets locaux

7.2.11.1 Utilisateurs et ordinateurs

Dans **Utilisateurs et ordinateurs**, vous pouvez filtrer la vue dans la zone de navigation à gauche en fonction des utilisateurs locaux ou rechercher des utilisateurs locaux donnés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la partie inférieure gauche de la fenêtre de navigation, cliquez sur **Filtrer**.
3. Sélectionnez **Utilisateur local** en tant que **Type**. Si vous recherchez un utilisateur particulier, saisissez son nom.
4. Cliquez sur l'icône de la loupe.

La vue **Utilisateurs et ordinateurs** est filtrée en fonction des critères.

Remarque : les comptes Microsoft sont toujours considérés comme des utilisateurs invités de SafeGuard Enterprise.

7.2.11.2 Consignation dans le journal

Les inscriptions réussies ou non des utilisateurs, des ordinateurs ou des groupes de travail sont consignées dans le journal. Vous pouvez consulter la liste de ces informations dans SafeGuard Management Center sous **Rapports** dans l'observateur d'événements.

7.3 Recherche d'utilisateurs, d'ordinateurs et de groupes dans la base de données SafeGuard Enterprise

Pour afficher des objets dans la boîte de dialogue **Rechercher des utilisateurs, ordinateurs et groupes**, vous avez besoin des droits en **Lecture seule** ou d'**Accès complet** pour les objets concernés.

Remarque : lorsque vous recherchez des objets, vous obtenez uniquement les résultats de la recherche sur les zones (domaines) sur lesquelles vous disposez de droits d'accès en tant que responsable de la sécurité. Seul un Responsable principal de la sécurité peut effectuer une recherche sur la racine.

Dans **Utilisateurs et ordinateurs**, vous pouvez rechercher des objets à l'aide de différents filtres. Par exemple, vous pouvez facilement identifier les doubles qui peuvent avoir été provoqués par un processus de synchronisation AD avec le filtre **Utilisateurs et ordinateurs dupliqués.** Ce filtre affiche tous les ordinateurs portant le même nom dans un domaine et tous les utilisateurs avec le même nom, nom de connexion ou nom de connexion avant 2000 dans un domaine.

Pour rechercher les objets :

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation **Utilisateurs et ordinateurs**, sélectionnez le conteneur requis.
3. Dans la barre de menus du SafeGuard Management Center, cliquez sur **Édition** > **Rechercher**.

   La boîte de dialogue **Rechercher des utilisateurs, ordinateurs et groupes** s'affiche.

4. Sélectionnez le filtre requis dans la liste déroulante **Rechercher**.
5. Dans le champ **Dans**, le conteneur sélectionné apparaît.

   Vous pouvez changer ceci en sélectionnant une option différente de la liste déroulante.

6. Si vous recherchez un objet spécifique, entrez le nom recherché dans le champ **Rechercher le nom**.
7. Avec la case à cocher **Supprimer les résultats après chaque recherche**, spécifiez si les résultats doivent être effacés après chaque processus de recherche.
8. Cliquez sur **Rechercher maintenant**.

Les résultats apparaissent dans la boîte de dialogue **Rechercher des utilisateurs, ordinateurs et groupes**. Si vous cliquez sur un des résultats dans cette boîte de dialogue, l'entrée correspondante est marquée dans l'arborescence **Utilisateurs et ordinateurs**. Si vous avez recherché les doublons par exemple, vous pouvez maintenant les supprimer facilement.

7.4 Affichage des propriétés d'objet dans Utilisateurs et ordinateurs

Pour afficher les propriétés d'objet, vous avez besoin des droits d'**Accès complet** ou en **Lecture seule** aux objets concernés.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, cliquez avec le bouton droit de la souris sur l'objet requis et sélectionnez **Propriétés**.

Les propriétés de l'objet sélectionné apparaissent. Si vous avez des droits d'accès en **Lecture seule** à l'objet en question, les informations sur les propriétés sont grisées dans la boîte de dialogue et vous ne pouvez pas les modifier.

8 Responsables de la sécurité de SafeGuard Enterprise

SafeGuard Enterprise peut être administré par un ou plusieurs responsables de la sécurité. La gestion basée sur le rôle de SafeGuard Enterprise permet de répartir l'administration entre plusieurs utilisateurs. Un utilisateur peut se voir attribuer un ou plusieurs rôles. Pour améliorer la sécurité, l'autorisation supplémentaire d'une action peut être attribuée au rôle d'un responsable.

Au cours de la configuration initiale du SafeGuard Management Center, un administrateur de niveau supérieur, le responsable principal de la sécurité, possédant tous les droits et un certificat, est créé par défaut. Par défaut, le certificat du responsable principal de la sécurité expire après 5 ans et peut être renouvelé dans la section **Responsables de la sécurité** du Management Center. D'autres responsables de la sécurité peuvent être attribués à des tâches spécifiques, comme le support ou l'audit.

Dans la zone de navigation du SafeGuard Management Center, vous pouvez réorganiser les responsables de la sécurité de façon hiérarchique pour refléter la structure organisationnelle de votre entreprise. Toutefois, cette hiérarchie ne tient pas compte des droits et des rôles.

Remarque : deux responsables de la sécurité ne doivent pas utiliser le même compte Windows sur le même ordinateur. Dans le cas contraire, il est impossible de distinguer correctement leurs droits d'accès. Une authentification supplémentaire ne peut être utile que lorsque les responsables de la sécurité doivent s'authentifier à l'aide de tokens/cartes à puce.

8.1 Rôles du responsable de la sécurité

Pour plus de simplicité, SafeGuard Enterprise propose des rôles prédéfinis pour les responsables de la sécurité dotés de diverses fonctions. Un responsable de la sécurité possédant les droits nécessaires peut également définir de nouveaux rôles à partir d'une liste d'actions/de droits et les attribuer à des responsables de la sécurité particuliers.

Les types de rôle suivants sont fournis :

- Rôle du responsable principal de la sécurité
- Rôles prédéfinis
- Rôles personnalisés

8.1.1 Responsable principal de la sécurité

Après avoir installé SafeGuard Enterprise, un responsable principal de la sécurité (MSO, Master Security Officer) est créé par défaut au cours de la configuration initiale du SafeGuard Management Center. Le responsable principal de la sécurité est un responsable de la sécurité de niveau supérieur. Il bénéficie de tous les droits et peut accéder à tous les objets (semblable à un administrateur Windows). Les droits du responsable principal de la sécurité ne peuvent pas être modifiés.

Plusieurs responsables principaux de la sécurité peuvent être créés pour une seule instance du SafeGuard Management Center. Pour des raisons de sécurité, la création d'au moins un MSO

supplémentaire est fortement recommandée. Les MSO supplémentaires peuvent être supprimés. Toutefois, il doit toujours rester un utilisateur bénéficiant du rôle de MSO et créé de manière explicite en tant que MSO dans la base de données SafeGuard Enterprise.

Un responsable principal de la sécurité peut déléguer des tâches à une autre personne. Pour ce faire, vous pouvez procéder de deux façons :

- Un nouveau responsable de la sécurité peut être créé dans **Responsables de la sécurité**.
- Un utilisateur ou tous les membres d'un conteneur importé d'Active Directory et visibles dans le répertoire racine du SafeGuard Management Center peuvent être promus au rang de responsable de la sécurité dans **Utilisateurs et ordinateurs**.

Un ou plusieurs rôles peuvent alors être attribués aux responsables de la sécurité. Par exemple, un utilisateur peut se voir attribuer le rôle de responsable supervision et celui de responsable du support.

Toutefois, le responsable principal de la sécurité peut également créer des rôles personnalisés et les attribuer à des utilisateurs particuliers.

8.1.2 Rôles prédéfinis

Dans le SafeGuard Management Center, les rôles de responsable de la sécurité suivants, sauf ceux du MSO, sont prédéfinis. L'attribution des droits à ces rôles prédéfinis ne peut être changée. Par exemple, si un rôle prédéfini possède le droit de "création d'éléments de stratégie et de groupes de stratégies", ce droit ne peut pas être supprimé du rôle. De même, un nouveau droit ne peut pas être ajouté à un rôle prédéfini. Toutefois, vous pouvez attribuer à tout moment une authentification responsable à des rôles prédéfinis.

- **Responsable supervision**

  Les responsables supervision peuvent accéder à leurs propres nœuds dans la zone **Responsables de la sécurité**. De même, ils sont autorisés à gérer les responsables de la sécurité inclus dans leurs nœuds respectifs.

- **Responsable de la sécurité**

  Les responsables de la sécurité possèdent des droits étendus, y compris des droits de configuration de SafeGuard Enterprise, de gestion des stratégies et des clés, ainsi que des autorisations relatives au contrôle et à la récupération.

- **Responsable support**

  Les responsables support ont le droit d'effectuer des actions de récupération. Ils peuvent également afficher la plupart des zones de fonctions du SafeGuard Management Center.

- **Responsable audit**

  Pour contrôle SafeGuard Enterprise, les responsables audit peuvent afficher la plupart des zones de fonctions du SafeGuard Management Center.

- **Responsable récupération**

  Les responsables récupération ont le droit de réparer la base de données SafeGuard Enterprise.

8.1.3 Rôles personnalisés

En tant que responsable de la sécurité possédant les droits nécessaires, vous pouvez définir de nouveaux rôles à partir d'une liste d'actions/de droits, puis les attribuer à un responsable de la sécurité existant ou nouveau. De même qu'avec les rôles prédéfinis, vous pouvez activer l'authentification responsable supplémentaire pour une fonction du rôle à tout moment.

Lors de l'attribution d'un nouveau rôle, notez les informations suivantes relatives à l'authentification supplémentaire :

Remarque : si un utilisateur a deux rôles avec les mêmes droits et si l'authentification supplémentaire est attribuée à l'un des rôles, elle s'applique automatiquement à l'autre également.

Un responsable de la sécurité avec les droits nécessaires peut ajouter des droits à un rôle personnalisé, ou en supprimer. Contrairement aux rôles prédéfinis, les rôles personnalisés peuvent être modifiés et même supprimés le cas échéant. Lorsque vous supprimez le rôle, il n'est plus attribué à aucun utilisateur. Si un seul rôle est attribué à un utilisateur et si ce rôle est supprimé, l'utilisateur ne peut plus se connecter au SafeGuard Management Center.

Remarque : le rôle et les actions définis dans le cadre de celui-ci déterminent ce qu'un utilisateur peut faire et ne pas faire. Ceci est également vrai si l'utilisateur a plusieurs rôles. Lorsque l'utilisateur s'est connecté au SafeGuard Management Center, les seules zones qui sont activées et affichées sont celles qui sont nécessaires pour son rôle respectif. Ceci s'applique également aux zones des scripts et de l'API. Il est donc important de toujours activer l'affichage de la zone dans laquelle les actions respectives sont définies. Les actions sont triées par zone de fonctions et disposées de manière hiérarchique. Cette structure permet de visualiser les actions nécessaires à l'exécution d'autres actions.

8.1.4 Authentification d'un responsable supplémentaire

L'authentification d'un responsable supplémentaire (également appelée "règle des deux personnes") peut être attribuée à des actions spécifiques d'un rôle. Cela signifie que l'utilisateur de ce rôle n'est autorisé à effectuer qu'une certaine action si un utilisateur d'un autre rôle est présent et le confirme. À chaque fois qu'un utilisateur effectue cette action, un autre utilisateur doit la confirmer.

Vous pouvez attribuer une authentification supplémentaire indifféremment à des rôles prédéfinis ou personnalisés. Dès que deux responsables minimum ont le même rôle, le rôle personnalisé peut également être sélectionné.

Le rôle consistant à effectuer l'autorisation supplémentaire doit être préalablement attribué à un utilisateur. De plus, la base de données SafeGuard Enterprise doit compter au moins deux responsables de la sécurité. Lorsqu'une action requiert une authentification supplémentaire, celle-ci est nécessaire même si l'utilisateur détient un autre rôle ne nécessitant pas d'authentification supplémentaire pour la même action.

Si un responsable crée un rôle alors qu'il ne possède pas le droit de modification de l'authentification supplémentaire, les paramètres relatifs à une authentification supplémentaire du nouveau rôle seront prérenseignés afin de correspondre à ceux définis pour le responsable de la création de ce rôle.

8.2 Création d'un rôle

Condition préalable : pour créer un rôle, vous devez posséder le droit d'affichage et de création de rôles de responsable de la sécurité. Pour attribuer une authentification supplémentaire, vous devez posséder le droit de "modification des paramètres d'authentification supplémentaire".

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Cliquez avec le bouton droit de la souris sur **Rôles personnalisés** et sélectionnez **Nouveau** > **Nouveau rôle personnalisé**.
3. Dans le champ **Nouveau rôle personnalisé**, saisissez un nom et une description pour le rôle.
4. Attribuez les actions à ce rôle : Sélectionnez les cases en regard de l'action requise dans la colonne **Activé**.

   Les actions sont triées par zone de fonctions et disposées de manière hiérarchique. Cette structure permet de visualiser les actions nécessaires à l'exécution d'autres actions.
5. Si nécessaire, attribuez une **Authentification d'un autre responsable** : Cliquez sur le paramètre par défaut **Aucune** et, depuis la liste, sélectionnez le rôle requis.

   Si un responsable crée un rôle sans posséder de droit de modification de l'authentification supplémentaire, les paramètres relatifs à l'authentification supplémentaire seront préalablement renseignés en fonction de l'authentification supplémentaire définie pour les rôles du responsable. Vous pouvez sélectionner une authentification supplémentaire si celle-ci a été définie pour plusieurs rôles du responsable.
6. Cliquez sur **OK**.

Le nouveau rôle est affiché sous **Rôles personnalisés** dans la fenêtre de navigation. Lorsque vous cliquez sur le rôle, les actions autorisées sont affichées dans la zone d'action de droite.

8.3 Attribution d'un rôle à un responsable de la sécurité

Condition préalable : pour attribuer un rôle, vous devez posséder le droit d'affichage et de modification des responsables de la sécurité.

1. Sélectionnez le responsable approprié dans la fenêtre de navigation.

   Les propriétés s'affichent dans la zone d'action de droite.
2. Attribuez les rôles nécessaires en sélectionnant les cases correspondantes en regard des rôles disponibles.

   Les rôles prédéfinis s'affichent en gras.
3. Cliquez sur le symbole à double flèche d'**Actualiser** dans la barre d'outils.

Le rôle est attribué au responsable de la sécurité.

Remarque : les rôles personnalisés complexes peuvent entraîner de légers problèmes de performances lors de l'utilisation de SafeGuard Management Center.

8.4 Affichage des propriétés du responsable et du rôle

Condition préalable : pour obtenir un aperçu des propriétés du responsable ou de l'attribution du rôle, vous devez posséder le droit d'affichage des responsables de la sécurité et des rôles de ces derniers.

Pour afficher les propriétés du responsable et du rôle :

1. Dans le SafeGuard Management Center, cliquez sur **Responsables de la sécurité**.
2. Dans la zone de navigation de gauche, cliquez deux fois sur l'objet dont vous souhaitez obtenir un aperçu.

Les informations disponibles dans la zone d'action à droite dépendent de l'objet sélectionné.

8.4.1 Affichage des propriétés du responsable principal de la sécurité

Les informations générales et de modification relatives au responsable principal de la sécurité s'affichent.

8.4.2 Affichage des propriétés des responsables de la sécurité

Les informations générales et de modification relatives au responsable de la sécurité s'affichent.

1. Dans **Propriétés**, sélectionnez l'onglet **Actions** afin d'afficher un résumé des actions autorisées et des rôles attribués au responsable de la sécurité.

8.4.3 Affichage des droits et des rôles des responsables de la sécurité

Un résumé des actions de tous les rôles attribués au responsable de la sécurité s'affiche. L'arborescence affiche les actions nécessaires à l'exécution d'autres actions. Les rôles attribués peuvent également être affichés.

1. Dans la boîte de dialogue <**Nom du responsable de la sécurité**> **Propriétés**, dans l'onglet **Actions**, sélectionnez une action pour afficher tous les rôles attribués qui contiennent cette action.
2. Cliquez deux fois sur un rôle dans la liste **Rôles attribués avec l'action sélectionnée**. La boîte de dialogue <**Nom du responsable de la sécurité**> **Propriétés** se ferme et les propriétés du rôle s'affichent.

8.4.4 Affichage des propriétés du rôle

Les informations générales et de modification relatives au rôle s'affichent.

1. Dans **Propriétés**, sélectionnez l'onglet **Attribution** afin d'afficher les responsables de la sécurité attribués à ce rôle.

8.4.5 Affichage de l'attribution du rôle

1. Dans <**Nom du rôle**> **Propriétés**, dans l'onglet **Attribution**, cliquez deux fois sur un responsable de la sécurité. La boîte de dialogue **Propriétés** se ferme et les données générales et les rôles du responsable de la sécurité s'affichent.

8.5 Modification d'un rôle

Vous pouvez effectuer les étapes suivantes :

- Modifier l'authentification supplémentaire uniquement.
- Modifier toutes les propriétés du rôle.

L'icône en regard des rôles affiche l'action disponible :

Icône	Description
	Le rôle peut être modifié (ajouter/supprimer des actions).
	L'authentification supplémentaire peut être modifiée.
	Les deux types de modification sont disponibles.

Remarque : vous ne pouvez pas modifier les rôles prédéfinis et les actions qui leur sont attribuées. Si une authentification supplémentaire est activée, celle-ci peut être modifiée pour tous les rôles, même les rôles prédéfinis.

8.5.1 Modification de l'authentification supplémentaire uniquement

Condition préalable : pour attribuer une authentification supplémentaire, vous devez posséder le droit d'affichage des rôles du responsable de la sécurité et de "modification des paramètres d'authentification supplémentaire".

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.

2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez sur le rôle à modifier. Dans la zone d'action de droite, cliquez sur le paramètre requis dans la colonne **Authentification de responsable de la sécurité supplémentaire** et sélectionnez un rôle différent dans la liste.

   Les rôles prédéfinis s'affichent en gras.

3. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

L'authentification responsable supplémentaire a été modifiée pour ce rôle.

8.5.2 Modification de toutes les propriétés d'un rôle

Condition préalable : pour modifier un rôle personnalisé, vous devez posséder le droit d'affichage et de modification des rôles de responsable de la sécurité. Pour attribuer de nouveau une authentification supplémentaire, vous devez posséder le droit de "modification des paramètres d'authentification supplémentaire".

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez avec le bouton droit de la souris sur le rôle à modifier et sélectionnez **Modifier un rôle personnalisé**.
3. Modifiez les propriétés selon vos besoins. Modifiez les propriétés d'authentification supplémentaire en cliquant sur la valeur de cette colonne et en sélectionnant le rôle requis.
4. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

Le rôle a été modifié.

8.6 Copie d'un rôle

Pour créer un rôle dont les propriétés sont identiques à celles d'un rôle existant, vous pouvez utiliser le rôle existant comme modèle pour le nouveau rôle. Vous pouvez sélectionner un rôle prédéfini ou personnalisé comme modèle.

Condition préalable : vous pouvez utiliser des rôles existants comme modèles uniquement si le responsable de la sécurité actuellement authentifié possède tous les droits contenus dans le modèle de rôle spécifique. Par conséquent, cette fonction peut ne pas être disponible pour les responsables ne possédant qu'un nombre d'actions limité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le rôle à copier et sélectionnez **Nouveau** > **Nouvelle copie du rôle**. Dans **Nouveau rôle personnalisé**, toutes les propriétés du rôle existant sont présélectionnées.
3. Saisissez un nouveau nom pour ce rôle et modifiez les propriétés selon les besoins.
4. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

Le nouveau rôle est créé.

8.7 Suppression d'un rôle

Remarque : les rôles prédéfinis ne peuvent pas être supprimés.

Condition préalable : pour supprimer un rôle, vous devez posséder le droit d'affichage et de suppression des rôles de responsable de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez avec le bouton droit sur le rôle à supprimer et sélectionnez **Supprimer**. En fonction des propriétés du rôle, un message d'avertissement spécifique s'affichera.

   Remarque : lorsque vous supprimez un rôle, tous les responsables de la sécurité auxquels ce rôle est attribué perdent ce dernier. Si le rôle est le seul attribué à un responsable de la sécurité, ce dernier ne peut plus se connecter au SafeGuard Management Center, sauf s'il se voit attribuer un nouveau rôle par un responsable de la sécurité supérieur. Si le rôle est utilisé à des fins d'authentification supplémentaire, le MSO devra effectuer une authentification supplémentaire.

3. Pour supprimer le rôle, cliquez sur **Oui** dans le message d'avertissement.
4. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

Le rôle est supprimé de la fenêtre de navigation et de la base de données.

8.8 Création d'un responsable principal de la sécurité

Condition préalable : pour créer un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de création de responsables de la sécurité.

Remarque : un moyen rapide de créer de nouveaux responsables principaux de la sécurité est de promouvoir un responsable de la sécurité. Retrouvez plus d'informations à la section Promotion des responsables de la sécurité à la page 49.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le nœud **Responsables principaux de la sécurité** et sélectionnez **Nouveau** > **Nouveau responsable principal de la sécurité**.

3. Saisissez les informations correspondantes dans **Nouveau responsable principal de la sécurité** :

Champ/case à cocher	Description
Activé	Le responsable de la sécurité peut être désactivé jusqu'à nouvel avis. Le responsable de la sécurité est dans le système mais ne peut pas encore se connecter au SafeGuard Management Center. Il peut seulement le faire et effectuer ses tâches d'administration lorsqu'un autre responsable l'active.
Nom	Saisissez le nom du responsable de sécurité tel qu'il est fourni dans les certificats créés par SafeGuard Enterprise sous la forme cn =. Le responsable de la sécurité est également affiché sous ce nom dans la fenêtre de navigation du SafeGuard Management Center. Ce nom doit être unique. Valeur maximale : 256 caractères
Description	Facultatif Valeur maximale : 256 caractères
Téléphone portable	Facultatif Valeur maximale : 128 caractères
E-Mail	Facultatif Valeur maximale : 256 caractères
Connexion au token	La connexion peut s'effectuer de la façon suivante : **Aucun token**. Le responsable de la sécurité ne peut pas se connecter avec un token. Il doit se connecter en saisissant les informations de connexion (nom d'utilisateur/mot de passe). **Facultatif** La connexion peut s'effectuer avec un token ou en saisissant les informations de connexion. Le responsable de la sécurité a le choix. **Obligatoire** un token doit être utilisé pour la connexion. Pour ce faire, la clé privée appartenant au certificat du responsable de la sécurité doit se trouver sur le token.

Champ/case à cocher	Description
Certificat	Un responsable de la sécurité a toujours besoin d'un certificat pour se connecter au SafeGuard Management Center. Le certificat peut être créé par SafeGuard Enterprise lui-même ou un certificat existant peut être utilisé. Si la connexion avec un token est essentielle, le certificat doit être ajouté au token du responsable de la sécurité. **Créer :** Le certificat et le fichier de clé sont créés et enregistrés dans un emplacement choisi. Saisissez et confirmez un mot de passe pour le fichier P12. Le fichier .p12 doit être à la disposition du responsable de la sécurité lorsqu'il se connecte. Le certificat créé est attribué automatiquement au responsable de la sécurité et affiché dans **Certificat**. Si des règles de mot de passe de SafeGuard Enterprise sont utilisées, celles-ci doivent être désactivées dans Active Directory. **Remarque :** longueur max. du chemin d'enregistrement et du nom de fichier : 260 caractères. Lors de la création d'un responsable de la sécurité, la partie publique du certificat suffit. Lors de la connexion au SafeGuard Management Center, cependant, la partie privée du certificat (le fichier de clé) est également requise. Si elle n'est pas disponible dans la base de données, elle doit l'être pour le responsable de la sécurité (sur une carte mémoire, par exemple), et peut être stockée dans le magasin de certificats pendant la connexion.
Certificat	**Importation :** Un certificat existant est utilisé et attribué au responsable de la sécurité lors de l'importation. Si l'importation s'effectue à partir d'un fichier de clé .p12, le mot de passe du certificat doit être connu. Si un conteneur de certificats PKCS#12 est sélectionné, tous les certificats sont chargés dans la liste de certificats attribuables. L'attribution du certificat s'effectue après l'importation, en le sélectionnant dans la liste déroulante.

4. Pour confirmer, cliquez sur **OK**.

Le nouveau responsable principal de la sécurité apparaît dans la fenêtre de navigation, sous le nœud **Responsables principaux de la sécurité**. Leurs propriétés peuvent être affichées en sélectionnant le responsable de la sécurité concerné dans la fenêtre de navigation. Le MSO peut se connecter au SafeGuard Management Center avec le nom affiché.

8.9 Création d'un responsable de la sécurité

Condition préalable : pour créer un responsable de la sécurité, vous devez posséder le droit d'affichage et de création de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.

2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le nœud du responsable de la sécurité où vous souhaitez placer le nouveau responsable de la sécurité, puis sélectionnez **Nouveau** > **Nouveau responsable de la sécurité**.

3. Procédez de la façon suivante dans la boîte de dialogue **Nouveau responsable de la sécurité** :

Champ/case à cocher	Description
Activé	Le responsable de la sécurité peut être désactivé jusqu'à nouvel avis. Le responsable de la sécurité est dans le système mais ne peut pas encore se connecter au SafeGuard Management Center. Il peut seulement le faire et effectuer ses tâches d'administration lorsqu'un autre responsable l'active.
Nom	Saisissez le nom du responsable de sécurité tel qu'il est fourni dans les certificats créés par SafeGuard Enterprise sous la forme cn =. Le responsable de la sécurité est également affiché sous ce nom dans la fenêtre de navigation du SafeGuard Management Center. Ce nom doit être unique. Valeur maximale : 256 caractères
Description	Facultatif Valeur maximale : 256 caractères
Téléphone portable	Facultatif Valeur maximale : 128 caractères
E-Mail	Facultatif Valeur maximale : 256 caractères
Validité	Sélectionnez les dates de début et de fin d'autorisation de connexion du responsable de la sécurité au SafeGuard Management Center.
Connexion au token	La connexion peut s'effectuer de la façon suivante: **Aucun token**. Le responsable de la sécurité ne peut pas se connecter avec un token. Il doit se connecter en saisissant ses informations de connexion (nom d'utilisateur/mot de passe). **Facultatif** La connexion peut s'effectuer avec un token ou en saisissant les informations de connexion. Le responsable de la sécurité a le choix. **Obligatoire** un token doit être utilisé pour la connexion. Pour ce faire, la clé privée appartenant au certificat du responsable de la sécurité doit se trouver sur le token.

Champ/case à cocher	Description
Certificat	Un responsable de la sécurité a toujours besoin d'un certificat pour se connecter au SafeGuard Management Center. Le certificat peut être créé par SafeGuard Enterprise lui-même ou un certificat existant peut être utilisé. Si la connexion avec un token est essentielle, le certificat doit être ajouté au token du responsable de la sécurité. **Créer :** Le certificat et le fichier de clé sont créés et enregistrés dans un emplacement choisi. Entrez et confirmez un mot de passe pour le fichier P12. Le fichier .p12 doit être à la disposition du responsable de la sécurité lorsqu'il se connecte. Le certificat créé est attribué automatiquement au responsable de la sécurité et affiché dans **Certificat**. Si des règles de mot de passe de SafeGuard Enterprise sont utilisées, celles-ci doivent être désactivées dans Active Directory. **Remarque :** longueur max. du chemin d'enregistrement et du nom de fichier : 260 caractères. Lors de la création d'un responsable de la sécurité, la partie publique du certificat suffit. Lors de la connexion au SafeGuard Management Center, cependant, la partie privée du certificat (le fichier de clé) est également requise. Si elle n'est pas disponible dans la base de données, elle doit l'être pour le responsable de la sécurité (sur une carte mémoire, par exemple), et peut être stockée dans le magasin de certificats pendant la connexion.
Certificat	**Importation :** Un certificat existant est utilisé et attribué au responsable de la sécurité lors de l'importation. Si l'importation s'effectue à partir d'un fichier de clé .p12, le mot de passe du certificat doit être connu. Si un conteneur de certificats PKCS#12 est sélectionné, tous les certificats sont chargés dans la liste de certificats attribuables. L'attribution du certificat s'effectue après l'importation, en le sélectionnant dans la liste déroulante.
Rôles du responsable de la sécurité	**Rôles** Des rôles prédéfinis ou personnalisés peuvent être attribués au responsable de la sécurité. Les droits associés à chaque rôle s'affichent sous **Action autorisée** dans la zone d'action en cliquant sur le rôle respectif ou en cliquant avec le bouton droit de la souris sur le responsable de la sécurité et en sélectionnant **Propriétés**, **Actions**. Il est possible d'attribuer plusieurs rôles à un utilisateur.

4. Pour confirmer, cliquez sur **OK**.

Le nouveau responsable de la sécurité apparaît dans la fenêtre de navigation, sous le nœud **Responsables de la sécurité** respectif. Leurs propriétés peuvent être affichées en sélectionnant le responsable de la sécurité concerné dans la fenêtre de navigation. Le responsable de la sécurité peut se connecter au SafeGuard Management Center avec le nom affiché. Vous devez ensuite

attribuer les objets/domaines de répertoire au responsable de la sécurité afin que celui-ci puisse exécuter ses tâches.

8.10 Attribution d'objets de répertoire à un responsable de la sécurité

Afin que les responsables de la sécurité puissent exécuter ses tâches, il doit posséder les droits d'accès aux objets de répertoire. Les droits d'accès peuvent être accordés aux domaines, aux unités organisationnelles (OU) et aux groupes d'utilisateurs ainsi qu'au nœud ".Autoregistered" situé sous le répertoire racine.

Dans **Utilisateurs et ordinateurs**, vous pouvez changer les droits d'accès d'un autre responsable de la sécurité si vous avez l'accès complet pour le conteneur approprié et êtes responsable du responsable de la sécurité en question. Vous ne pouvez pas changer vos propres droits d'accès. Si vous attribuez un responsable de la sécurité à un objet de répertoire pour la première fois, le responsable de la sécurité hérite de vos droits d'accès pour ce conteneur.

Remarque : vous ne pouvez pas accorder à d'autres responsables de la sécurité des droits d'accès plus élevés que vos propres droits d'accès.

Condition préalable : si vous voulez accorder/refuser au responsable de la sécurité le droit d'accéder aux objets de répertoire et de les gérer, vous devez posséder les droits "utilisateurs et ordinateurs" "d'affichage des droits d'accès des responsables de la sécurité" et "d'autoriser/de refuser l'accès au répertoire". En plus, vous avez besoin des droits d'**Accès complet** pour les objets de répertoire en question.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, sélectionnez les objets de répertoire requis.

   Remarque : l'arborescence n'affiche que les objets de répertoire pour lesquels vous avez les droits d'accès. Si vous avez des droits d'**Accès complet**, l'objet apparaît en noir. Les objets avec un accès en **Lecture seule** apparaissent en bleu. Un nœud grisé n'est pas accessible mais apparaît quand même, s'il existe des nœuds au-dessous auxquels vous avez accès.

3. Dans la zone d'action de droite, cliquez sur l'onglet **Accès**.
4. Pour attribuer les droits pour les objets sélectionnés, faites glisser le responsable requis depuis l'extrémité droite dans le tableau **Accès**.
5. Dans la colonne **Droits d'accès**, sélectionnez les droits que vous voulez accorder au responsable de la sécurité pour les objets sélectionnés :

   - **Accès complet**
   - **Lecture seule**
   - **Refusé**

   Pour annuler l'attribution des droits pour les objets sélectionnés, faites glisser le responsable de la sécurité en retour dans le tableau **Responsables**.

6. Pour enregistrer les modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

Les objets sélectionnés sont disponibles pour le responsable de la sécurité correspondant.

Remarque : si deux responsables de la sécurité travaillent sur la même base de données SafeGuard Enterprise en même temps et si l'un d'entre eux change ses droits d'accès, un message

apparaît pour informer l'autre responsable de la sécurité et tous les changements non enregistrés sont perdus. Si un responsable de la sécurité perd complètement les droits d'accès pour un nœud, l'accès n'est plus accordé et un message approprié apparaît. La fenêtre de navigation est actualisée en conséquence.

8.10.1 Affichage des droits du responsable de la sécurité pour les objets du répertoire

Les droits d'accès attribués aux responsables de la sécurité pour les objets du répertoire sont affichés sur l'onglet **Accès** des objets correspondants dans **Utilisateurs et ordinateurs**.

Remarque : l'onglet **Accès** n'affiche que les droits d'accès pour les conteneurs auxquels vous avez les droits d'accès. De la même façon, il n'affiche que les responsables de la sécurité dont vous êtes responsable.

L'onglet **Accès** affiche les informations suivantes :

- La colonne **Responsables** affiche les types et les noms des responsables de la sécurité qui ont été attribués aux objets du répertoire.
- La colonne **Attribué par** affiche la manière dont le responsable de la sécurité a reçu les droits d'accès :
- La **Date d'attribution**
- La colonne **Droits d'accès** affiche les droits accordés : **Accès complet**, **Refusé** ou en **Lecture seule**.
- La colonne **Origine** indique le nom complet du nœud où le droit d'accès a été attribué au responsable correspondant. Par exemple : Si le droit a été attribué à un nœud parent de l'objet de répertoire sélectionné, le nœud parent apparaît ici. Dans ce cas, le responsable de la sécurité a hérité du droit d'accès pour l'objet de répertoire sélectionné par l'attribution à son nœud parent.
- La colonne **État** affiche comment le responsable de la sécurité a reçu le droit d'accès :
  - **Hérité** (couleur bleue du texte) : Le droit d'accès a été hérité d'un nœud parent.
  - **Remplacé** (couleur marron du texte) : Le droit d'accès a été hérité d'un nœud parent, mais a changé au nœud sélectionné par attribution directe.
  - **Directement affecté** (couleur noire du texte) : Le droit d'accès a été attribué directement au nœud sélectionné.

  Pour les droits hérités, vous pouvez afficher une infobulle dans la colonne **État** indiquant l'origine du droit correspondant.

8.11 Promotion des responsables de la sécurité

Procédez comme suit :

- Élevez un utilisateur au grade de responsable de la sécurité dans la zone **Utilisateurs et ordinateurs**.

- Élevez un responsable de la sécurité au grade de responsable principal de la sécurité dans la zone **Responsables de la sécurité**.

8.11.1 Conditions préalables à la promotion d'un utilisateur

Un responsable de la sécurité avec les droits nécessaires peut promouvoir des utilisateurs au rang de responsables de la sécurité et leur attribuer des rôles.

Les responsables de la sécurité ainsi créés peuvent se connecter au SafeGuard Management Center avec leurs codes d'accès Windows ou leur code PIN de token/carte à puce. Ils peuvent travailler et être gérés comme tout autre responsable de la sécurité.

Les conditions préalables suivantes doivent être remplies :

- Les utilisateurs à promouvoir doivent avoir été importés depuis un Active Directory et être visibles dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center.
- Pour permettre à un utilisateur promu de se connecter au SafeGuard Management Center en tant que responsable de la sécurité, un certificat utilisateur est nécessaire. Vous pouvez créer ce certificat lors de la promotion d'un utilisateur. Retrouvez plus d'informations à la section Promotion d'un utilisateur au rang de responsable de la sécurité à la page 50. Pour rendre possible la connexion avec les codes d'accès Windows, le fichier.p12 contenant la clé privée doit se trouver dans la base de données SafeGuard Enterprise. Pour se connecter avec un code PIN de token ou de carte à puce, le fichier.p12 contenant la clé privée doit se trouver sur le token ou la carte à puce.

  Remarque : si vous créez le certificat lors de la promotion d'un utilisateur, ce dernier va devoir utiliser le mot de passe du certificat pour se connecter au SafeGuard Management Center. Il va devoir saisir le mot de passe du certificat même s'il est invité à saisir le mot de passe Windows. Ceci s'applique également lors de la connexion à SafeGuard Enterprise Web Help Desk.

8.11.2 Promotion d'un utilisateur au rang de responsable de la sécurité

Condition préalable : pour promouvoir un utilisateur, vous devez être responsable principal de la sécurité ou responsable de la sécurité avec les droits nécessaires.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Cliquez avec le bouton droit sur l'utilisateur que vous souhaitez promouvoir au rang de responsable de la sécurité et sélectionnez **Faire de cet utilisateur un responsable de la sécurité**.
3. L'étape suivante est différente selon qu'un certificat utilisateur est disponible ou non pour l'utilisateur sélectionné.
   - Si un certificat utilisateur a déjà été attribué à cet utilisateur, la boîte de dialogue **Sélection d'un ou des rôles** apparaît. Passez à l'étape 4.

- Si aucun certificat utilisateur est disponible, un message apparaît vous demandant si une paire de clés à signature automatique doit être créée pour cet utilisateur. Cliquez sur **Oui** et saisissez et confirmez un mot de passe dans la boîte de dialogue **Mot de passe pour le nouveau certificat**. Maintenant, la boîte de dialogue **Sélection du ou des rôles** apparaît.

4. Dans la boîte de dialogue **Sélection du ou des rôles**, sélectionnez les rôles requis et cliquez sur **OK**.

L'utilisateur est désormais promu et apparaît dans la zone **Responsables de la sécurité** avec son nom d'utilisateur. Leurs propriétés peuvent être affichées en sélectionnant le responsable concerné dans la fenêtre de navigation. La clé privée de l'utilisateur est stockée dans la base de données et l'option **Aucun token** est activée. L'option **Facultatif** est activée si la clé privée de l'utilisateur est sur le token ou sur la carte à puce.

Si nécessaire, vous pouvez faire glisser le responsable de la sécurité à la position requise dans l'arborescence **Responsables de la sécurité**.

Le responsable de la sécurité peut se connecter au SafeGuard Management Center avec le nom affiché.

8.11.3 Promotion d'un responsable de la sécurité au rang de responsable principal de la sécurité

Condition préalable : pour promouvoir un responsable de la sécurité, vous devez posséder le droit d'affichage et de modification de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable de la sécurité à promouvoir et sélectionnez **Promouvoir au rang de responsable principal de la sécurité**.
3. Si le responsable promu possède des enfants, vous êtes invité à sélectionner un nouveau nœud parent pour les enfants.

Le responsable de la sécurité a été promu et apparaît sous le nœud **Responsables principaux de la sécurité**. En tant que responsable principal de la sécurité, le responsable promu recevra tous les droits sur l'ensemble des objets. Par conséquent, il perdra tous les droits attribués ainsi que l'accès au domaine autorisé de manière individuelle dans **Utilisateur et ordinateurs**.

8.12 Rétrogradation de responsables principaux de la sécurité

Condition préalable : Pour rétrograder des responsables principaux de la sécurité au rang de responsable de la sécurité, vous devez être responsable principal de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le responsable principal de la sécurité que vous voulez rétrograder et sélectionnez **Rétrograder au rang de responsable de la sécurité**.
3. Vous êtes invité à sélectionner un nœud parent pour le responsable et à attribuer au moins un rôle.

Le responsable de la sécurité a été rétrogradé et s'affiche sous le nœud **Responsables de la sécurité** sélectionné. Le responsable ainsi rétrogradé perd tous ses droits sur l'ensemble des objets et ne reçoit que ceux attribués à son ou ses rôles. Un responsable rétrogradé ne possède aucun droit sur les domaines. Vous devez accorder individuellement des droits d'accès dans la zone **Utilisateurs et ordinateurs**, sous l'onglet **Accès**.

8.13 Modification du certificat du responsable de la sécurité

Condition préalable : pour modifier le certificat d'un responsable de la sécurité ou d'un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de modification des responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez sur le responsable de la sécurité dont vous souhaitez modifier le certificat. Le certificat actuellement attribué apparaît dans la zone d'action de droite, dans le champ **Certificats**.
3. Dans la zone d'action, cliquez sur la liste déroulante **Certificats** et sélectionnez un certificat différent.
4. Pour enregistrer les modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

8.14 Organisation des responsables de la sécurité dans l'arborescence

Vous pouvez organiser les responsables de la sécurité de manière hiérarchique dans la fenêtre de navigation **Responsables de la sécurité** et ce, afin de représenter la structure organisationnelle de votre société.

L'arborescence peut être organisée pour l'ensemble des responsables de la sécurité, à l'exception des responsables principaux de la sécurité. Les responsables principaux de la sécurité sont affichés dans une liste à un niveau, sous le nœud Responsable principal de la sécurité (MSO). Le nœud des responsables de la sécurité comporte une arborescence dans laquelle chaque nœud représente un responsable de la sécurité. Toutefois, cette hiérarchie ne tient pas compte des droits et des rôles.

Condition préalable : pour déplacer un responsable de la sécurité dans l'arborescence, vous devez posséder le droit d'affichage et de modification de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, faites glisser le responsable que vous souhaitez déplacer vers le nœud approprié.

Tous les enfants du responsable sélectionné seront également déplacés.

8.15 Basculement rapide de responsables de la sécurité

À titre pratique, vous pouvez redémarrer rapidement SafeGuard Management Center afin de vous connecter sous le nom d'un autre responsable.

1. Dans SafeGuard Management Center, sélectionnez **Fichier** > **Changer le responsable**. SafeGuard Management Center redémarre et la boîte de dialogue de connexion s'affiche.
2. Sélectionnez le responsable de la sécurité que vous souhaitez connecter au SafeGuard Management Center, puis saisissez son mot de passe. Si vous travaillez en mode mutualisé (Multi Tenancy), vous serez connecté selon la même configuration de base de données.

SafeGuard Management Center redémarre et la vue attribuée au responsable connecté s'affiche.

8.16 Suppression d'un responsable de la sécurité

Condition préalable : pour supprimer un responsable de la sécurité ou un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de suppression de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable de la sécurité ou le responsable principal de la sécurité à supprimer et sélectionnez **Supprimer**. Vous ne pouvez pas supprimer le responsable de la sécurité sous le nom duquel vous êtes connecté.
3. Si le responsable possède des enfants, vous êtes invité à sélectionner un nouveau nœud parent pour les enfants.

Le responsable est supprimé de la base de données.

Remarque : un responsable principal de la sécurité explicitement créé en tant que responsable et non seulement promu au rang de responsable de la sécurité doit cependant être conservé dans la base de données. Si un utilisateur promu au rang de responsable de la sécurité est supprimé de la base de données, son compte utilisateur l'est également.

Remarque : si le responsable à supprimer s'est vu attribuer un rôle incluant une authentification supplémentaire et si le responsable est le seul à qui ce rôle a été attribué, le responsable sera tout de même supprimé. Nous considérons que le responsable principal de la sécurité sera en mesure de prendre le contrôle de l'autorisation supplémentaire.

9 Clés et certificats

Lors de l'importation de la structure du répertoire, SafeGuard Enterprise dans sa configuration par défaut génère automatiquement des clés pour :

- Domaines
- Conteneurs/OU

et les attribue aux objets correspondants. Des clés d'ordinateur et d'utilisateur sont générées selon les besoins.

Clés pour les groupes

Dans a configuration par défaut, SafeGuard Enterprise ne génère pas automatiquement de clés pour les groupes. Ce comportement est désactivé par défaut. En tant que responsable de la sécurité, vous pouvez changer ce comportement sur l'onglet **Clés** en sélectionnant **Outils** > **Options**. Si **Groupes** est coché sur l'onglet **Clés**, SafeGuard Enterprise génère automatiquement des clés de groupe, lorsque la base de données est synchronisée. En bas de l'onglet **Synchronisation**, il est indiqué pour quels éléments des clés sont générées lors de la synchronisation.

Les clés ne peuvent pas être supprimées. Elles sont conservées en permanence dans la base de données de SafeGuard Enterprise.

Lorsqu'un ordinateur d'extrémité est démarré pour la première fois, SafeGuard Enterprise lui génère une clé d'ordinateur (clé machine définie).

Remarque : la clé machine définie est uniquement générée lorsque le chiffrement de volume est installé sur l'ordinateur d'extrémité.

Chaque utilisateur obtient toutes ses clés lors de la connexion à partir de son jeu de clés. Le jeu de clés utilisateur comporte les éléments suivants :

- Les clés des groupes auxquels appartient l'utilisateur ;
- Les clés des conteneurs/OU globaux des groupes auxquels appartient l'utilisateur.

Les clés du jeu de clés de l'utilisateur déterminent les données auxquelles l'utilisateur peut accéder. L'utilisateur ne peut accéder qu'aux données pour lesquelles il possède une clé spécifique.

Remarque : pour éviter que trop de clés de groupes non utilisées apparaissent dans le jeu de clés de l'utilisateur, vous pouvez spécifier les clés à cacher. Retrouvez plus d'informations à la section Masquage des clés à la page 56.

Pour afficher toutes les clés d'un utilisateur, cliquez sur **Utilisateurs et ordinateurs** et sélectionnez l'onglet **Clés**.

Pour afficher toutes les clés, cliquez sur **Clés et certificats** dans le SafeGuard Management Center et sélectionnez **Clés**. Vous pouvez générer des listes de **Clés attribuées** et de **Clés inactives**.

Remarque : la liste **Certificats attribués** indique seulement les clés attribuées aux objets pour lesquels vous avez des droits en **Lecture seule** ou d'**Accès complet**. La vue **Clés** indique le

nombre de clés disponibles, quels que soient vos droits d'accès. La liste **Clés attribuées** indique le nombre de clés visibles en fonction de vos droits d'accès.

1. Cliquez sur **Utilisateurs et ordinateurs** pour ouvrir l'affichage.
2. Les clés d'un objet sélectionné sont affichées dans la zone action et dans les vues respectives.
3. L'affichage dans la zone d'action dépend des sélections dans la zone de navigation. Toutes les clés attribuées à l'objet sélectionné sont affichées.
4. Sous **Clés disponibles**, toutes les clés disponibles s'affichent. Les clés déjà attribuées à l'objet sélectionné sont grisées. Sélectionnez **Filtre** pour basculer entre des clés déjà attribuées à un objet (actives) et des clés non attribuées à un objet (inactives).

Après l'importation, chaque utilisateur reçoit un certain nombre de clés utilisables pour le chiffrement des données.

9.1 Clés pour le chiffrement des données

Des clés sont attribuées aux utilisateurs pour le chiffrement de volumes spécifiques lors de la définition de stratégies du type **Protection des périphériques**.

Dans une stratégie de type **Protection des périphériques**, vous pouvez spécifier le paramètre **Clé à utiliser pour le chiffrement** pour chaque support.

Ici, vous pouvez décider quelles sont les clés que l'utilisateur peut ou doit utiliser pour le chiffrement:

- **Toute clé du jeu de clés utilisateur**

  Après s'être connectés à Windows, les utilisateurs peuvent sélectionner les clés qu'ils souhaiteraient utiliser pour chiffrer un volume particulier. Une boîte de dialogue s'affiche pour permettre aux utilisateurs de sélectionner la clé de leur choix.

- **Toute clé du jeu de clés utilisateur sauf la clé utilisateur**

  Les utilisateurs ne sont pas autorisés à utiliser leurs clés personnelles pour chiffrer des données.

- **Toute clé de groupe du jeu de clés utilisateur**

  Les utilisateurs ne peuvent sélectionner qu'une des clés de groupe présentes dans leur jeu de clés.

- **Clé machine définie**

  C'est la clé unique générée exclusivement pour cet ordinateur par SafeGuard Enterprise lors du premier démarrage. L'utilisateur n'a pas d'autre option. Une clé machine définie est généralement utilisée par la partition d'initialisation et système et pour les unités sur lesquelles se trouve le répertoire Documents and Settings.

- **Clé définie dans la liste**

  Cette option permet de définir une clé particulière que l'utilisateur doit utiliser pour le chiffrement. Pour indiquer une clé d'utilisateur de cette manière, veuillez définir une clé sous **Clé définie pour le chiffrement**. Cette option s'affiche une fois que vous sélectionnez **Clé définie sur la liste**.

Cliquez sur le bouton [**...**] situé en regard de **Clé définie pour le chiffrement** pour afficher une boîte de dialogue dans laquelle vous pouvez spécifier une clé. Assurez-vous que l'utilisateur a aussi la clé correspondante.

Marquez la clé sélectionnée et cliquez sur **OK**. La clé sélectionnée sera utilisée pour le chiffrement sur l'ordinateur client.

9.1.1 Attribution de clés dans Utilisateurs et ordinateurs

Pour attribuer des clés aux utilisateurs, vous avez besoin des droits d'**Accès complet** pour l'objet concerné.

Pour attribuer une nouvelle clé aux utilisateurs :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'objet requis (par exemple, utilisateur, groupe ou conteneur).
3. Cliquez avec le bouton droit de la souris sur l'onglet **Clés** et sélectionnez **Attribuer une nouvelle clé** dans le menu contextuel.
4. Dans la boîte de dialogue **Attribution d'une nouvelle clé** :
   a) Saisissez un **Nom symbolique** et une **Description** pour la clé.
   b) Pour masquer la clé dans le jeu de clés de l'utilisateur, sélectionnez la case à cocher **Masquer la clé**.
5. Cliquez sur **OK**.

La clé est attribuée et affichée dans l'onglet **Clé**.

9.1.2 Masquage des clés

Pour éviter que trop de clés de groupes non utilisées apparaissent dans le jeu de clés d'un utilisateur sur l'ordinateur d'extrémité, vous pouvez spécifier les clés à masquer. Les clés qui n'apparaissent pas dans le jeu de clés de l'utilisateur peuvent quand même être utilisées pour accéder aux fichiers chiffrés, mais pas pour en chiffrer des nouveaux.

Pour masquer les clés :

1. Dans le SafeGuard Management Center, cliquez sur **Clés et certificats**.
2. Dans la zone de navigation, cliquez sur **Clés** et sélectionnez **Clés attribuées**.

   La vue **Clés attribuées** apparaît affichant la colonne **Masquer la clé**.
3. Il existe deux moyens de spécifier que les clés doivent être masquées :
   - Sélectionnez la case à cocher dans la colonne **Masquer la clé** de la clé requise.
   - Sélectionnez une ou plusieurs clés et cliquez avec le bouton droit de la souris pour ouvrir un menu contextuel.

     Sélectionnez **Masquer la clé à l'utilisateur**.

4. Enregistrez vos changements dans la base de données.

Les clés indiquées n'apparaissent pas dans le jeu de clés de l'utilisateur.

Retrouvez plus d'informations sur l'affichage du jeu de clés de l'utilisateur sur l'ordinateur d'extrémité dans le *Manuel d'utilisation de SafeGuard Enterprise*, au chapitre *Icône de la barre d'état système et infobulles*.

Remarque : si une stratégie indique une clé masquée à utiliser pour le chiffrement, le paramètre **Masquer la clé** n'affecte pas le chiffrement sur l'ordinateur d'extrémité.

9.2 Clés personnelles pour le chiffrement basé sur fichier par le File Share

Une clé personnelle est un type particulier de chiffrement créé pour un utilisateur donné qui ne peut pas être partagé avec d'autres utilisateurs. Une clé personnelle qui est active pour un utilisateur donné est appelée une clé personnelle active. Les clés personnelles actives ne peuvent pas être attribuées à d'autres utilisateurs.

Dans les stratégies **File Encryption**, vous pouvez définir des règles de chiffrement qui utilisent l'espace réservé **Clé personnelle** au lieu d'un nom de clé. Pour de telles règles, la clé de chiffrement à utiliser est la clé personnelle active de l'utilisateur.

Lorsque vous définissez une règle de chiffrement pour que le chemin *C:\encrypt* soit chiffré avec la clé personnelle, des clés différentes sont utilisées pour différents utilisateurs. Vous pouvez ainsi vous assurer que les informations dans les dossiers spécifiques sont privées pour les utilisateurs. Retrouvez plus d'informations sur File Share à la section Utilisation de File Encryption avec File Share à la page 165.

Si une File Encryption définit une clé personnelle à utiliser pour le chiffrement, des clés personnelles sont créées automatiquement pour les utilisateurs correspondants, s'ils n'ont pas encore de clés personnelles actives.

En tant que responsable de la sécurité avec les droits requis, vous pouvez créer des clés personnelles pour des utilisateurs sélectionnés ou pour tous les utilisateurs de groupes sélectionnés dans le SafeGuard Management Center. Vous pouvez aussi rétrograder des clés personnelles actives, par exemple lorsqu'un utilisateur quitte la société.

9.2.1 Création automatique de clés personnelles

Si une règle de chiffrement File Encryption définit une clé personnelle à utiliser pour le chiffrement et si l'utilisateur n'a pas encore de clé personnelle active, le serveur SafeGuard Enterprise la crée automatiquement. Lors du délai entre la réception de la stratégie sur l'ordinateur d'extrémité et la mise à disposition de la clé personnelle active requise, l'utilisateur n'est pas autorisé à créer de nouveaux fichiers dans les dossiers couverts par la règle File Encryption.

Pour un déploiement initial des stratégies **File Encryption** avec des règles de chiffrement à l'aide de clés personnelles sur un groupe plus important d'utilisateurs (des centaines ou plus) qui n'ont pas encore de clés personnelles actives, nous conseillons de créer les clés personnelles dans SafeGuard Management Center (retrouvez plus d'informations à la section Création de

clés personnelles pour plusieurs utilisateurs à la page 58). La charge sur le serveur SafeGuard Enterprise sera réduite.

9.2.2 Création d'une clé personnelle pour un utilisateur unique

Pour créer une clé personnelle, vous avez besoin des droits **Créer des clés** et **Attribuer des clés**. En plus, vous avez besoin des droits d'**Accès complet** pour l'objet en question. Pour remplacer une clé personnelle active, vous avez besoin du droit **Gérer les clés personnelles**.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'utilisateur requis.
3. Cliquez avec le bouton droit de la souris sur l'onglet **Clés** et sélectionnez **Attribuer une nouvelle clé** dans le menu contextuel.
4. Dans la boîte de dialogue **Attribution d'une nouvelle clé** :
   a) Saisissez une description pour la clé personnelle.
   b) Pour cacher la clé personnelle dans le jeu de clés de l'utilisateur, sélectionnez **Masquer la clé**.
5. Selon que vous créez une clé personnelle pour un utilisateur qui n'a pas encore de clé personnelle active ou pour un utilisateur qui en a une, la boîte de dialogue **Attribution d'une nouvelle clé** affiche des cases à cocher différentes. Sélectionnez la case à cocher affichée, pour définir la clé nouvellement créée comme une clé personnelle :
   - **Clé personnelle** : cette case à cocher apparaît pour les utilisateurs qui n'ont pas encore de clé personnelle active.
   - **Remplacer la clé personnelle active** : cette case à cocher apparaît pour les utilisateurs qui ont déjà une clé personnelle active.
6. Cliquez sur **OK**.

La clé personnelle est créée pour l'utilisateur sélectionné. Dans l'onglet**Clé**, la clé apparaît comme la **Clé personnelle active** pour l'utilisateur. Pour un utilisateur qui avait déjà une clé personnelle active, la clé existante est rétrogradée et l'utilisateur en reçoit une nouvelle. La clé personnelle rétrogradée reste dans le jeu de clés de l'utilisateur. La clé personnelle active ne peut pas être attribuée à d'autres utilisateurs.

9.2.3 Création de clés personnelles pour plusieurs utilisateurs

Pour créer des clés personnelles, vous avez besoin des droits **Créer des clés** et **Attribuer des clés**. En plus, vous avez besoin des droits d'**Accès complet** pour les objets en question. Pour remplacer des clés personnelles actives existantes, vous avez besoin du droit **Gérer les clés personnelles**.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, cliquez avec le bouton droit de la souris sur le nœud pour lequel vous voulez créer des clés personnelles :
   - un nœud de domaine,
   - le nœud .Autoregistered à la racine ou dans les domaines ou

- un nœud Unité Organisationnelle.

3. Dans le menu contextuel, sélectionnez **Créer des clés personnelles pour les utilisateurs**.
4. Dans la boîte de dialogue **Créer des clés personnelles pour les utilisateurs** :
   a) Saisissez une description pour les clés personnelles.
   b) Pour cacher les clés personnelles dans les jeux de clés des utilisateurs, sélectionnez **Masquer la clé**.
   c) Pour remplacer les clés personnelles actives existantes par les nouvelles, sélectionnez **Remplacer les clés personnelles actives existantes**.
5. Cliquez sur **OK**.

Les clés personnelles sont créées comme pour tous les utilisateurs du nœud sélectionné. Dans l'onglet**Clé**, les clés apparaissent comme des **Clés personnelles actives** pour les utilisateurs. Si les utilisateurs avaient déjà des clés personnelles actives et si vous avez sélectionné **Remplacer les clés personnelles actives existantes**, les clés existantes sont rétrogradées et les utilisateurs en reçoivent des nouvelles. Les clés personnelles rétrogradées restent dans les jeux de clés des utilisateurs. Les clés personnelles actives individuelles ne peuvent pas être attribuées à d'autres utilisateurs.

9.2.4 Rétrogradation des clés personnelles actives

Pour rétrograder manuellement des clés personnelles actives, vous avez besoin des droits **Modifier des clés** et **Gérer des clés personnelles**. Par défaut, le droit **Gérer des clés personnelles** a été attribué au rôle prédéfini de responsable principal de la sécurité, mais il peut aussi être attribué aux nouveaux rôles définis par l'utilisateur. En plus, vous avez besoin des droits d'**Accès complet** pour l'objet en question.

Vous pouvez rétrograder manuellement des clés personnelles actives, par exemple si un utilisateur quitte la société. Dans la mesure où vous avez le droit **Gérer des clés personnelles**, vous pouvez attribuer la clé personnelle rétrogradée de cet utilisateur à d'autres utilisateurs pour leur donner un accès en lecture seule aux fichiers chiffrés avec cette clé. Mais ils ne peuvent pas utiliser cette clé pour le chiffrement des fichiers.

Remarque : ceci ne peut pas être annulé. Une clé personnelle rétrogradée ne peut jamais devenir une clé personnelle active quel que soit l'utilisateur.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'utilisateur requis.
3. Dans l'onglet **Clé**, cliquez avec le bouton droit de la souris sur la **Clé personnelle active** requise et sélectionnez **Rétrograder la clé personnelle** dans le menu contextuel.

La clé est rétrogradée. C'est encore une clé personnelle, mais elle ne peut plus être utilisée comme clé personnelle active. Si une règle File Encryption définit une clé personnelle à utiliser pour le chiffrement et si l'utilisateur n'a pas encore de clé personnelle active, le serveur SafeGuard Enterprise la crée automatiquement.

9.3 Certificats

- Un seul certificat peut être affecté par utilisateur. Si ce certificat utilisateur est stocké sur un token, les utilisateurs peuvent donc utiliser ce token (token cryptographique - Kerberos) pour se connecter à leur ordinateur d'extrémité.
- Notez que lors de l'importation d'un certificat utilisateur, la section publique et la section privée de ce certificat sont importées toutes les deux. Si uniquement la partie publique est importée, seule l'authentification par token est prise en charge.
- La combinaison des certificats AC et de la CRL (Certificate Revocation List, liste de révocation des certificats) doit correspondre. Dans le cas contraire, les utilisateurs ne peuvent pas se connecter à leurs ordinateurs respectifs. Vérifiez que la combinaison est correcte. SafeGuard Enterprise n'effectue pas cette vérification.
- Si des certificats de l'autorité de certification (AC) sont supprimés dans la base de données et si vous ne souhaitez plus les utiliser, veuillez les supprimer manuellement du magasin local de tous les ordinateurs administrateurs.

  SafeGuard Enterprise peut ensuite uniquement communiquer avec les certificats ayant expiré si les clés nouvelles et anciennes sont présentes sur le même token.
- Les certificats de l'AC ne peuvent pas provenir d'un token et être stockés dans la base de données ou dans le magasin de certificats. Si vous utilisez des certificats de l'AC, ces derniers doivent être disponibles sous forme de fichiers et pas seulement sous forme de token. Ceci s'applique également aux CRL.
- Les certificats générés par SafeGuard Enterprise sont signés avec SHA-1 ou SHA-256 pour vérification. SHA-256 fournit une sécurité optimale et il est utilisé par défaut sur toutes les premières installations. Si la version 6 de SafeGuard Enterprise ou une version précédente doit tout de même être gérée ou si la mise à niveau a lieu à partir d'une version antérieure, l'algorithme SHA-1 est utilisé par défaut.
- Les certificats fournis par le client et importés dans SafeGuard Enterprise ne sont actuellement pas vérifiés conformément à RFC3280. Par exemple, nous n'empêchons pas l'utilisation de certificats de signature à des fins de chiffrement.
- Les certificats de connexion des responsables de la sécurité doivent se trouver dans le "magasin de certificats MY".

Remarque : la liste **Certificats attribués** dans **Clés et certificats** indique seulement les certificats attribués aux objets pour lesquels vous avez des droits en **Lecture seule** ou d'**Accès complet**. La vue **Certificat** indique le nombre de certificats disponibles, quels que soient vos droits d'accès. La liste **Certificats attribués** indique le nombre de certificats disponibles en fonction de vos droits d'accès.

Pour modifier les certificats, vous avez besoin des droits d'**Accès complet** au conteneur dans lequel résident les utilisateurs.

9.3.1 Importation des certificats d’autorité de certification et des listes de révocation de certificats

Si des certificats AC (autorité de certification) sont utilisés, veuillez importer toute la hiérarchie AC, y compris toutes les listes de révocation des certificats dans la base de données SafeGuard. Les certificats AC ne peuvent pas être récupérés à partir de tokens. Ils doivent être mis à disposition sous la forme de fichier afin que vous puissiez les importer dans la base de données SafeGuard Enterprise. Ceci s'applique également aux listes de révocation de certificats.

1. Dans le SafeGuard Management Center, cliquez sur **Clés et certificats**.
2. Sélectionnez **Certificats** et cliquez sur l'icône **Importer les certificats de l'AC** de la barre d'outils. Naviguez jusqu'aux fichiers du certificat AC que vous souhaitez importer.

   Les certificats importés s'affichent dans la zone d'action de droite.
3. Sélectionnez **Certificats** et cliquez sur l'icône **Importer la liste de révocation de certificats** de la barre d'outils. Naviguez jusqu'aux fichiers de la liste de révocation de certificats que vous souhaitez importer.

   Les listes de révocation de certificats importées s'affichent dans la zone d'action de droite.
4. Vérifiez que l'AC et la liste de révocation de certificats sont correctes. Les certificats de l'AC doivent correspondre à la liste de révocation de certificats pour que les utilisateurs puissent se connecter aux ordinateurs concernés. SafeGuard Enterprise n'effectue pas cette vérification.

9.3.2 Modification de l'algorithme pour les certificats autosignés

Conditions préalables : tous les composants SafeGuard Enterprise doivent être à la version 6.1.

Par défaut, les certificats générés par SafeGuard Enterprise (entreprise, machine, responsable de la sécurité et utilisateur) sont signés par l'algorithme **SHA-256** à la première installation pour une sécurité optimale.

Lors de la mise à niveau à partir de SafeGuard Enterprise 6 ou d'une version antérieure, l'algorithme **SHA-1** est automatiquement utilisé pour les certificats autosignés. Vous pouvez le modifier manuellement sur **SHA-256** pour une sécurité optimale suite à la mise à niveau.

Remarque : modifiez uniquement l'algorithme sur **SHA-256** si tous les composants et ordinateurs d'extrémité SafeGuard Enterprise ont été mis à niveau à la version en cours. **SHA-256** n'est pas pris en charge dans les environnements mixtes. Par exemple, les ordinateurs d'extrémité SafeGuard Enterprise 6 sont administrés par SafeGuard Management Center 6.1. Si vous avez un environnement mixte, vous devez effectuer cette tâche et ne pas modifier l'algorithme sur **SHA-256**.

La modification de l'algorithme pour les certificats autosignés s'effectue de la manière suivante :

- Modification de l'algorithme.
- Création d'un ordre de modification du certificat (CCO, Certificate Change Order).
- Création d'un package de configuration contenant le CCO.

- Redémarrage des serveurs (base de données) SafeGuard Enterprise.
- Distribution et déploiement des packages de configuration sur les ordinateurs d'extrémité.

Pour modifier l'algorithme pour les certificats autosignés :

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Options.**
2. Dans l'onglet **Général**, sous **Certificats**, sélectionnez l'algorithme nécessaire dans **Algorithme de hachage pour les certificats générés** et cliquez sur **OK**.
3. Dans l'onglet **Certificats**, sous **Demander**, cliquez sur **Mettre à jour**. Dans la boîte de dialogue **Mettre à jour le certificat d'entreprise**, saisissez un nom de CCO et indiquez un chemin de sauvegarde. Saisissez un mot de passe pour le fichier P12 et retapez-le. En option, saisissez un commentaire et cliquez sur **Créer**.
4. Lorsque vous y êtes invité, veuillez confirmer que vous êtes bien conscient que cette modification ne peut pas être annulée et que tous les packages de configuration créés après la mise à jour de ce certificat d'entreprise ont besoin que ce CCO soit inclus pour être exploités sur les ordinateurs d'extrémité déjà installés.
5. Lorsque vous y êtes invité, veuillez confirmer que la mise à jour a réussi et qu'un CCO à inclure dans tous les packages de configuration a été créé. Cliquez sur **OK**.
6. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**
7. Sélectionnez le type de package de configuration des ordinateurs d'extrémité : **Packages du client administré** ou **Packages du client autonome**.
8. Cliquez sur **Ajouter un package de configuration** et saisissez un nom pour le package de configuration.
9. Sélectionnez le **CCO** que vous aviez créé auparavant.
10. Procédez à toutes les autres sélections de votre choix.
11. Indiquez un chemin de sortie pour le package de configuration (MSI).
12. Cliquez sur **Créer un package de configuration**.

    Le package de configuration (MSI) a été créé dans le répertoire spécifié.

13. Redémarrez tous les serveurs (base de données) SafeGuard Enterprise.
14. Distribuez ce package aux ordinateurs d'extrémité SafeGuard Enterprise protégés et déployez-le sur ceux-ci.

Tous les certificats générés par SafeGuard Enterprise sont signés avec le nouvel algorithme.

Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/116791.aspx.

9.4 Exportation du certificat d'entreprise et du responsable principal de la sécurité

Dans une installation SafeGuard Enterprise, les deux éléments suivants sont essentiels et doivent être sauvegardés dans un emplacement sûr :

- Le certificat d'entreprise enregistré dans la base de données SafeGuard.

- Le certificat du responsable principal de la sécurité (MSO) se trouvant dans le magasin de certificats de l'ordinateur sur lequel le SafeGuard Management Center est installé.

Vous pouvez exporter ces deux certificats sous la forme de fichiers .p12 à des fins de sauvegarde. Pour restaurer les installations, vous pouvez importer le certificat d'entreprise et du responsable de la sécurité correspondant sous la forme de fichiers .p12 et les utiliser lorsque vous paramétrez une nouvelle base de données. Ceci pour éviter de restaurer l'intégralité de la base de données.

Remarque : nous vous conseillons de réaliser cette tâche immédiatement après la configuration initiale du SafeGuard Management Center.

9.4.1 Exportation des certificats d'entreprise

Remarque : seuls les responsables principaux de la sécurité sont autorisés à exporter les certificats d'entreprise à des fins de sauvegarde.

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Options.**
2. Cliquez sur l'onglet **Certificats**, puis sur **Exporter** dans la section **Certificat d'entreprise**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Saisissez un mot de passe, confirmez-le, puis cliquez sur **OK**.
4. Saisissez un nom et un emplacement de stockage pour le fichier, puis cliquez sur **OK**.

Le certificat d'entreprise est exporté sous la forme d'un fichier .p12 à l'emplacement désigné et peut être utilisé à des fins de récupération.

9.4.2 Exportation du certificat du responsable principal de la sécurité

Pour sauvegarder le certificat du responsable principal de la sécurité connecté au SafeGuard Management Center :

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Options.**
2. Sélectionnez l'onglet **Certificats** et cliquez sur **Exporter** dans la section **Certificat de <administrateur>**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Saisissez un mot de passe, confirmez-le, puis cliquez sur **OK**.
4. Saisissez un nom et un emplacement de stockage pour le fichier à exporter et cliquez sur **OK**.

Le certificat du responsable principal de la sécurité actuellement connecté est exporté sous la forme d'un fichier .p12 à l'emplacement défini et peut être utilisé à des fins de récupération.

9.5 Clients virtuels

Remarque : les clients virtuels peuvent uniquement être utilisés pour le **Chiffrement intégral du disque SafeGuard avec authentification au démarrage SafeGuard**.

Les clients virtuels sont des fichiers de clés spécifiques pouvant être utilisés pour la récupération lors d'une procédure Challenge/Réponse lorsque les informations requises sur l'utilisateur ne

sont pas disponibles et lorsque la procédure Challenge/Réponse n'est généralement pas prise en charge (par exemple, lorsque l'authentification au démarrage SafeGuard est corrompue).

Pour activer une procédure Challenge/Réponse dans cette situation de récupération complexe, des fichiers spécifiques appelés clients virtuels peuvent être créés. Ils doivent être distribués à l'utilisateur avant que la session Challenge/Réponse ne soit exécutée. À l'aide de clients virtuels, la procédure Challenge/Réponse peut être lancée avec un outil de récupération de clé sur l'ordinateur d'extrémité. Il suffit ensuite à l'utilisateur d'informer le responsable support de la ou des clés requises et de saisir le code de réponse afin de pouvoir accéder à nouveau aux volumes chiffrés.

La récupération est possible à l'aide soit d'une seule clé, soit d'un fichier de clé chiffré contenant plusieurs clés.

La zone **Clés et certificats** du SafeGuard Management Center vous permet d'effectuer les tâches suivantes :

- Créer et exporter des clients virtuels.
- Créer et exporter des fichiers de clés chiffrés contenant plusieurs clés.
- Afficher et filtrer des clients virtuels et des fichiers de clés exportés.
- Supprimer des clients virtuels.

9.5.1 Création de clients virtuels

Les fichiers de clients virtuels peuvent être utilisés par différents ordinateurs et pour plusieurs sessions de Challenge/Réponse.

1. Dans SafeGuard Management Center, cliquez sur **Clés et certificats**.
2. Dans la fenêtre de navigation de gauche, cliquez sur **Clients virtuels**.
3. Dans la barre d'outils, cliquez sur **Ajouter un client virtuel**.
4. Saisissez un nom unique de client virtuel et cliquez sur **OK**.

   Les clients virtuels sont identifiés dans la base de données par ces noms.
5. Dans la barre d'outils, cliquez sur l'icône **Enregistrer** pour enregistrer le client virtuel dans la base de données.

Le nouveau client virtuel apparaît dans la zone d'action.

9.5.2 Exportation de clients virtuels

Une fois le client virtuel créé, vous devez l'exporter dans un fichier. Ce fichier est toujours nommé **`recoverytoken.tok`** et doit être distribué au support. Ce fichier doit être disponible dans l'environnement de l'ordinateur d'extrémité pour lancer une session Challenge/Réponse avec un outil de récupération(par exemple, lorsque l'authentification au démarrage SafeGuard est corrompue). L'utilisateur doit placer le fichier de client virtuel,

`recoverytoken.tok`, dans le même dossier que l'outil de récupération pour la prise en charge d'une procédure Challenge/Réponse.

1. Dans le SafeGuard Management Center, cliquez sur **Clés et certificats**.
2. Dans la fenêtre de navigation de gauche, cliquez sur **Clients virtuels**.
3. Dans la zone d'action, recherchez le client virtuel concerné en cliquant sur la loupe. Les clients virtuels disponibles apparaissent.
4. Sélectionnez l'entrée requise dans la zone d'action et cliquez sur **Exporter le client virtuel** dans la barre d'outils.
5. Sélectionnez l'emplacement de stockage du fichier **`recoverytoken.tok`** et cliquez sur **OK**. Un message indiquant que l'opération a réussi apparaît.
6. Distribuez ce fichier de client virtuel, **`recoverytoken.tok`**, aux utilisateurs de SafeGuard Enterprise concernés.

Conservez ce fichier en lieu sûr, sur une carte mémoire par exemple. Dans le cadre d'une procédure Challenge/Réponse, ce fichier doit se trouver dans le même dossier que l'outil de récupération.

9.5.3 Création et exportation de fichiers de clés pour la récupération des clients virtuels

Lorsque plusieurs clés sont requises pour pouvoir de nouveau accéder à des volumes chiffrés lors de la récupération d'un client virtuel, le responsable de la sécurité peut les combiner dans un fichier exporté. Ce fichier de clé est chiffré à l'aide d'un mot de passe aléatoire, qui est stocké dans la base de données. Ce mot de passe est propre à chaque fichier de clé créé.

Le fichier de clé chiffré doit être transmis à l'utilisateur et l'utilisateur doit l'avoir au démarrage d'une session Challenge/Réponse avec un outil de récupération.

Dans la session Challenge/Réponse, le mot de passe du fichier de clé est transmis avec le code de réponse. Le fichier de clé peut alors être déchiffré avec le mot de passe et tous les volumes chiffrés avec les clés disponibles sont de nouveau accessibles.

Pour exporter les fichiers de clés, vous avez besoin des droits d'**Accès complet** pour les objets auxquels les clés correspondantes sont attribuées.

1. Dans le SafeGuard Management Center, cliquez sur **Clés et certificats**.
2. Dans la fenêtre de navigation de gauche, cliquez sur **Clients virtuels** puis sur **Fichiers de clés exportés**.
3. Dans la barre d'outils, cliquez sur **Exporter des clés dans un fichier de clé**.

4. Dans **Exporter des clés dans un fichier de clé**, entrez les informations suivantes :
   a) **Répertoire** : Cliquez sur [**...**] pour sélectionner l'emplacement du fichier de clé.
   b) **Nom du fichier** : Le fichier de clé est chiffré à l'aide d'un mot de passe aléatoire qui s'affiche dans **Nom du fichier**. Vous ne pouvez pas modifier ce nom.
   c) Cliquez sur **Ajouter une clé** ou sur **Supprimer une clé** pour ajouter ou supprimer des clés. Une fenêtre contextuelle s'affiche pour rechercher et sélectionner les clés requises. Cliquez sur **OK** pour confirmer la sélection.
   d) Cliquez sur **OK** pour confirmer toutes les saisies.
5. Distribuez le fichier de clé dans l'environnement respectif des ordinateurs d'extrémité. Il doit être disponible avant que le code de réponse ne soit saisi sur l'ordinateur d'extrémité.

9.5.4 Affichage et filtrage des vues Client virtuel

Pour trouver plus facilement le client virtuel ou les clés demandés lors d'un Challenge/Réponse, il existe plusieurs possibilités de filtrage et de recherche dans SafeGuard Management Center sous **Clés et certificats**.

9.5.5 Vues des clients virtuels

1. Cliquez sur **Clients virtuels** dans la fenêtre de navigation de gauche.
2. Cliquez sur la loupe pour générer la liste complète de tous les clients virtuels.
3. Filtrez les clients virtuels par **Nom symbolique** ou par **GUID de clé**.

9.5.6 Vues des fichiers de clés exportés

1. Dans SafeGuard Management Center, cliquez sur **Clients virtuels** puis sur **Fichiers de clés exportés**.
2. Cliquez sur la loupe pour générer la liste complète de tous les fichiers de clés exportés.
3. Cliquez sur l'icône + située en regard du fichier de clé requis pour afficher les clés contenues dans ce fichier.

9.5.7 Suppression de clients virtuels

1. Ouvrez SafeGuard Management Center et cliquez sur **Clés et certificats**.
2. Cliquez sur **Clients virtuels** dans la fenêtre de navigation de gauche.
3. Dans la zone d'action, recherchez le client virtuel concerné en cliquant sur la loupe. Les clients virtuels disponibles apparaissent.
4. Sélectionnez l'entrée requise dans la zone d'action et cliquez sur **Supprimer le client virtuel** dans la barre d'outils.
5. Enregistrez les modifications dans la base de données en cliquant sur l'icône **Enregistrer** de la barre d'outils.

Le client virtuel est supprimé de la base de données.

10 Ordres de modification du certificat d'entreprise

Les ordres de modification du certificat d'entreprise (CCO, Company Certificate Change Orders) sont utilisés dans les cas suivants :

- **Renouvellement du certificat d'entreprise** en cas d'expiration.

  Le renouvellement du certificat d'entreprise est possible pour les ordinateurs d'extrémité administrés et les ordinateurs d'extrémité autonomes. Il peut uniquement être activé à partir de la console d'administration.

- **Déplacement des ordinateurs d'extrémité non administrés** dans un environnement différent. Par exemple, si vous avez deux environnements Sophos SafeGuard différents et souhaitez les fusionner en un environnement Sophos SafeGuard unique au sein duquel l'un des deux environnements devra toujours être l'environnement cible.

  Vous pouvez effectuer ceci en échangeant le certificat d'entreprise des ordinateurs d'extrémité d'un environnement par le certificat d'entreprise de l'environnement cible.

  Remarque : seuls les responsables principaux de la sécurité sont autorisés à créer des ordres de modification du certificat d'entreprise (CCO). Pour permettre à d'autres responsables de la sécurité de créer des ordres de modification du certificat d'entreprise, le Responsable principal de la sécurité doit créer un rôle personnalisé et attribuer le droit **Gérer les CCO** à ce rôle.

10.1 Renouvellement du certificat d'entreprise

Un certificat d'entreprise sur le point d'expirer peut être renouvelé dans le SafeGuard Management Center. À la connexion, SafeGuard Management Center commence à afficher un avertissement six mois avant l'expiration du certificat d'entreprise. Sans certificat d'entreprise valide, un ordinateur d'extrémité ne peut pas se connecter au serveur. Le renouvellement du certificat d'entreprise comprend trois étapes :

- La création d'un ordre de modification du certificat (CCO, Certificate Change Order)
- La création d'un package de configuration contenant le CCO
- Le redémarrage des serveurs et la distribution et le déploiement des packages de configuration sur les systèmes d'extrémité.

Pour renouveler un certificat d'entreprise :

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Options.**
2. Sélectionnez l'onglet **Certificats** et cliquez sur **Mettre à jour** dans la section **Demander**.
3. Dans la boîte de dialogue **Mettre à jour le certificat d'entreprise**, saisissez un nom de CCO et indiquez un chemin de sauvegarde. Saisissez un mot de passe pour le fichier P12 et retapez-le. En option, saisissez un commentaire et cliquez sur **Créer**.

4. Lorsque vous y êtes invité, veuillez confirmer que vous êtes bien conscient que cette modification ne peut pas être annulée et que tous les packages de configuration créés après la mise à jour de ce certificat d'entreprise ont besoin que ce CCO soit inclus pour être exploités sur les ordinateurs d'extrémité déjà installés.
5. Lorsque vous y êtes invité, veuillez confirmer que la mise à jour a réussi et qu'un CCO à inclure dans tous les packages de configuration a été créé. Cliquez sur **OK**.
6. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**
7. Sélectionnez **Packages du client administré**.
8. Cliquez sur **Ajouter un package de configuration** et saisissez un nom pour le package de configuration.
9. Attribuez un **Serveur principal** (le **serveur secondaire** n'est pas nécessaire).
10. Sélectionnez le **CCO** que vous avez créé auparavant pour mettre à jour le certificat d'entreprise.
11. Sélectionnez le mode **Chiffrement du transport** définissant comment chiffrer la connexion entre le client SafeGuard Enterprise et le serveur SafeGuard Enterprise : chiffrement Sophos ou SSL.

    Le protocole SSL présente l'avantage d'être standard et de permettre d'établir une connexion plus rapidement qu'en utilisant le chiffrement de transport SafeGuard. Le chiffrement SSL est sélectionné par défaut. Retrouvez plus d'informations sur la sécurisation des connexions de transport avec SSL dans le *Guide d'installation de SafeGuard Enterprise*.
12. Indiquez un chemin de sortie pour le package de configuration (MSI).
13. Cliquez sur **Créer un package de configuration**.

    Si vous avez sélectionnez le chiffrement SSL en tant que mode de **Chiffrement du transport**, la connexion au serveur est validée. En cas d'échec de la connexion, un message d'avertissement s'affiche.

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Assurez-vous de redémarrer tous les serveurs SGN. Vous devez maintenant distribuer ce package aux ordinateurs d'extrémité SafeGuard Enterprise administrés et le déployer sur ceux-ci.

10.2 Remplacement du certificat d'entreprise

Le remplacement du certificat d'entreprise est nécessaire lorsque vous voulez déplacer un ordinateur d'extrémité d'un environnement autonome à un autre différent. L'ordinateur d'extrémité à déplacer doit avoir le certificat d'entreprise de l'environnement dans lequel il va être déplacé. Sinon, le système d'extrémité n'accepte pas les stratégies du nouvel environnement. Les tâches requises pour remplacer le certificat d'entreprise peuvent être exécutées dans le SafeGuard Management Center et dans le SafeGuard Policy Editor. Dans la description suivante, le terme 'outil d'administration' sert à signifier à la fois le SafeGuard Management Center et le SafeGuard Policy Editor, car le remplacement du certificat d'entreprise est identique dans les deux cas.

Les conditions préalables suivantes doivent être remplies :

Sachez quel est votre environnement Management Center/Policy Editor source et cible. Le Management Center/Policy Editor source est celui que vous avez utilisé pour la création des

packages de configuration pour les ordinateurs d'extrémité qui sont à déplacer. Le Management Center/Policy Editor cible est celui vers lequel les ordinateurs d'extrémité seront déplacés.

Pour remplacer le certificat d'entreprise :

1. Dans l'outil de gestion cible, exportez le certificat d'entreprise : Dans le menu **Outils**, cliquez sur **Options**. Sélectionnez l'onglet **Certificats** et cliquez sur le bouton **Exporter** sous **Certificat d'entreprise**. Saisissez et confirmez un mot de passe pour la sauvegarde du certificat lorsque vous y êtes invité et sélectionnez un répertoire de destination et un nom de fichier également lorsque vous y êtes invité. Le certificat d'entreprise est exporté (fichier cer).
2. Dans l'outil d'administration d'origine, allez dans le menu **Outils**, et cliquez sur **Options**. Sélectionnez l'onglet **Certificats** et cliquez sur **Créer...** dans la section **Demander**. Dans la boîte de dialogue **Créer un CCO**, recherchez le certificat d'entreprise cible que vous avez exporté dans l'outil d'administration cible (étape 1). Assurez-vous qu'il s'agit du certificat désiré. Cliquez sur **Créer** et sélectionnez un répertoire de destination et un nom de fichier pour le fichier .cco. Confirmez que vous voulez placer un **Ordre de modification du certificat d'entreprise**. Sachez qu'un CCO n'est pas relié à des ordinateurs d'extrémité spécifiques. À l'aide d'un CCO, tout client de l'environnement source peut être déplacé.
3. Dans l'outil d'administration cible, veuillez importer le CCO créé dans l'outil d'administration source. Dans le menu **Outils**, cliquez sur **Outil de package de configuration** et sélectionnez l'onglet **CCO**. Cliquez sur **Importer**.
4. Dans la boîte de dialogue **Importer un CCO**, sélectionnez le CCO que vous avez créé dans l'outil d'administration source et saisissez un nom de CCO et, si vous le souhaitez, une description. Cliquez sur **OK**.
5. Dans l'outil d'administration cible, créez un nouveau package de configuration : Dans le menu **Outils**, cliquez sur **Outil de package de configuration** > **Packages du client autonome** et ajoutez un nouveau package de configuration. Sélectionnez le CCO importé dans le menu déroulant dans la colonne **CCO**. Spécifiez un emplacement sous **Chemin de sortie du package de configuration**. Cliquez sur **Créer un package de configuration**. Le package de configuration est créé dans l'emplacement spécifié.
6. Installez ce package de configuration sur tous les ordinateurs d'extrémité que vous voulez déplacer de l'environnement source vers l'environnement cible.

10.3 Gestion des ordres de modification du certificat d'entreprise

Dans le SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Outil de package de configuration**. Tous les ordres de modification du certificat d'entreprise (CCO, Company Certificate Change Order) apparaissent dans l'onglet **CCO**.

Des informations détaillées sur le CCO sélectionné apparaissent dans la partie inférieure de la boîte de dialogue.

Si le CCO a été créé pour mettre à jour le certificat d'entreprise, le **Certificat d'entreprise d'origine** doit être renouvelé. Si le CCO a été créé pour déplacer les ordinateurs d'extrémité, vous devez déplacer le certificat d'entreprise de l'environnement des ordinateurs d'extrémité à déplacer dans un nouvel environnement.

Le **Certificat d'entreprise de destination** est le nouveau certificat d'entreprise dans le cas où le CCO a été créé pour mettre à jour le certificat d'entreprise ou le certificat d'entreprise de l'environnement dans lequel les systèmes d'extrémité doivent être déplacés.

Au-dessous des détails du certificat, on peut voir pour quelles tâches le CCO sélectionné peut être utilisé.

Remarque : pour pouvoir gérer les CCO, vous devez disposer du droit de **Gérer les CCO**.

10.3.1 Importation

Lors de la création de packages de configuration, avant de pouvoir sélectionner un CCO ayant été créé par un autre outil d'administration afin de modifier le certificat d'entreprise, vous devez importer ce CCO.

Si vous cliquez sur **Importer...**, une boîte de dialogue s'ouvre dans laquelle vous pouvez sélectionner et nommer le CCO. Le nom que vous saisissez ici apparaît sur l'onglet **CCO** de l'**Outil de package de configuration**.

10.3.2 Exportation

À l'aide de la fonctionnalité **Exporter**, les CCO stockés dans la base de données peuvent être exportés et sont alors disponibles sous la forme de fichiers .cco.

11 Utilisation de stratégies

Les sections suivantes décrivent les tâches administratives relatives aux stratégies, par exemple la création, le regroupement et la sauvegarde.

Remarque : pour l'attribution, la suppression ou la modification des stratégies,vous avez besoin des droits d'**Accès complet** aux objets appropriés ainsi qu'à tout groupe activé pour les stratégies données.

Retrouvez une description détaillée de tous les paramètres de stratégie disponibles dans SafeGuard Enterprise à la section Paramètres de stratégie à la page 111.

11.1 Création de stratégies

1. Connectez-vous au SafeGuard Management Center avec le mot de passe défini lors de la configuration initiale.
2. Dans la zone de navigation, cliquez sur **Stratégies**.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis sélectionnez **Nouveau**.
4. Sélectionnez le type de stratégie.

   Une boîte de dialogue permettant de nommer la nouvelle stratégie s'affiche.

5. Saisissez un nom et éventuellement une description de la nouvelle stratégie.

   Stratégies de protection des périphériques :

   Si vous créez une stratégie de protection du périphérique, spécifiez d'abord la cible de la protection du périphérique. Les cibles possibles sont les suivantes :

   - Stockage de masse (volumes d'initialisation/autres volumes)
   - Supports amovibles
   - Lecteurs optiques
   - Modèles de périphériques de stockage
   - Périphériques de stockage distincts
   - Stockage dans le Cloud

   Une stratégie distincte doit être créée pour chaque cible. Vous pouvez ultérieurement combiner les stratégies individuelles dans un groupe de stratégies nommé *Chiffrement* par exemple.

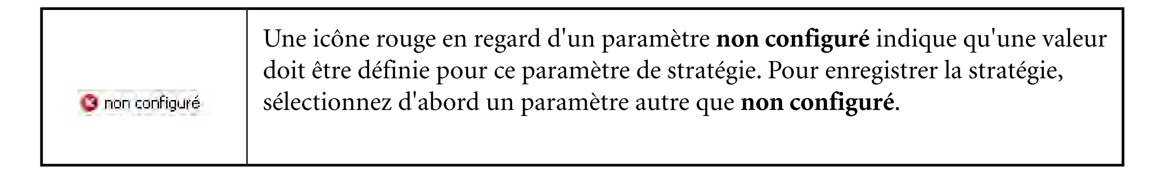
6. Cliquez sur **OK**.

La nouvelle stratégie s'affiche dans la fenêtre de navigation sous **Éléments de stratégie**. Dans la zone d'action, tous les paramètres du type de stratégie sélectionné s'affichent et peuvent être changés.

11.2 Édition des paramètres de stratégie

Lors de la sélection d'une stratégie dans la fenêtre de navigation, vous pouvez éditer les paramètres de la stratégie dans la zone d'action.

Remarque :



non configuré	Une icône rouge en regard d'un paramètre **non configuré** indique qu'une valeur doit être définie pour ce paramètre de stratégie. Pour enregistrer la stratégie, sélectionnez d'abord un paramètre autre que **non configuré**.

Restauration des valeurs par défaut de paramètres de stratégie

Dans la barre d'outils, les icônes suivantes servent à la configuration des paramètres de stratégie :

Icône	Paramètre de stratégie
	Affiche les valeurs par défaut des paramètres de stratégie qui n'ont pas été configurés (paramètre **non configuré**). Les valeurs par défaut pour les paramètres des stratégies sont affichés par défaut. Cliquez sur l'icône pour masquer les valeurs par défaut.
	Définit le paramètre de stratégie défini sur **non configuré**.
	Définit tous les paramètres de stratégie d'une zone sur **non configuré**.
	Définit la valeur par défaut de la stratégie marquée.
	Définit tous les paramètres de stratégie d'une zone sur la valeur par défaut.

Différences entre les stratégies spécifiques d'une machine et les stratégies spécifiques d'un utilisateur

Stratégie de couleur bleue	La stratégie s'applique uniquement aux machines et non aux utilisateurs.
Stratégie de couleur noire	La stratégie s'applique aux machines et aux utilisateurs.

11.3 Groupes de stratégies

Les stratégies SafeGuard Enterprise peuvent être combinées dans des groupes de stratégies. Un groupe de stratégies peut contenir différents types de stratégies. Dans SafeGuard Management Center, le groupe de stratégies **Par défaut** disponible est attribué à la **Racine** sous **Utilisateurs et ordinateurs**.

Si vous rassemblez des stratégies du même type dans un groupe, les paramètres sont fusionnés automatiquement. Dans ce cas, vous pouvez définir des priorités d'utilisation des paramètres. Les paramètres d'une stratégie ayant une priorité supérieure remplacent ceux d'une stratégie de priorité inférieure.

Un paramètre de stratégie défini remplace les paramètres des autres stratégies, si

- la stratégie avec ce paramètre a une priorité supérieure.
- le paramètre de stratégie n'a pas encore été défini (**non configuré**).

Remarque : les stratégies se chevauchant attribuées à un groupe peuvent aboutir à un calcul incorrect des priorités. Assurez-vous d'utiliser des paramètres de stratégie disjonctifs.

Exception relative à la protection du périphérique :

Les stratégies de protection des périphériques sont fusionnées uniquement si elles ont été définies pour la même cible (volume d'initialisation, par exemple). Les paramètres sont ajoutés si elles désignent des cibles différentes.

11.3.1 Combinaison de stratégies dans des groupes

Condition préalable : les stratégies individuelles de différents types doivent être tout d'abord créées.

1. Dans la zone de navigation, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Groupes de stratégies** et sélectionnez **Nouveau**.
3. Cliquez sur **Nouveau groupe de stratégies**. Une boîte de dialogue pour nommer le groupe de stratégies s'affiche.
4. Entrez le nom et éventuellement la description du groupe de stratégies. Cliquez sur **OK**.
5. Le nouveau groupe de stratégies s'affiche dans la fenêtre de navigation sous **Groupes de stratégies**.

6. Sélectionnez le groupe de stratégies. La zone d'action indique tous les éléments requis pour regrouper les stratégies.
7. Pour ajouter les stratégies au groupe, glissez-les de la liste de stratégies disponibles dans la zone de stratégies.
8. Vous pouvez définir une **priorité** pour chaque stratégie en les organisant grâce au menu contextuel.

   Si vous rassemblez des stratégies du même type dans un groupe, les paramètres sont fusionnés automatiquement. Dans ce cas, vous pouvez définir des priorités d'utilisation des paramètres. Les paramètres d'une stratégie ayant une priorité supérieure remplacent ceux d'une stratégie de priorité inférieure. Si une option est définie sur **non configuré**, le paramètre n'est **pas remplacé** dans une stratégie de priorité inférieure.

   Exception relative à la protection du périphérique :

   Les stratégies de protection des périphériques sont fusionnées uniquement si elles ont été définies pour la même cible (volume d'initialisation, par exemple). Les paramètres sont ajoutés si elles pointent des cibles différentes.
9. Enregistrez la stratégie avec **Fichier** > **Enregistrer**.

Le groupe de stratégies contient désormais les paramètres de toutes les stratégies individuelles.

11.3.2 Résultats du regroupement de stratégies

Le résultat du regroupement de stratégies s'affiche séparément.

Pour afficher le résultat, cliquez sur l'onglet **Résultat**.

- Un onglet distinct s'affiche pour chaque type de stratégie.

  Les paramètres obtenus de la combinaison des stratégies individuelles dans un groupe s'affichent.

- Pour les stratégies de protection du périphérique, un onglet s'affiche pour chaque cible de stratégie (volumes d'initialisation, lecteur X, etc.).

11.4 Sauvegarde de stratégies et de groupes de stratégies

Vous pouvez créer des sauvegardes de stratégies et de groupes de stratégies sous forme de fichiers XML. Si nécessaire, les stratégies/groupes de stratégies correspondants peuvent ensuite être restaurés à partir de ces fichiers XML.

1. Dans la fenêtre de navigation, sélectionnez la stratégie/le groupe de stratégies sous **Éléments de stratégie** ou **Groupes de stratégies**.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Sauvegarder la stratégie**.

   Remarque : la commande **Sauvegarder la stratégie** est également accessible dans le menu **Actions**.

3. Dans la boîte de dialogue **Enregistrer sous**, entrez le nom du fichier XML, puis sélectionnez un emplacement de stockage. Cliquez sur **Enregistrer**.

La sauvegarde de la stratégie/du groupe de stratégies est stockée sous forme de fichier XML dans le répertoire spécifié.

11.5 Restauration de stratégies et de groupes de stratégies

Pour restaurer une stratégie/un groupe de stratégies à partir d'un fichier XML:

1. Dans la fenêtre de navigation, sélectionnez **Éléments de stratégie/Groupes de stratégies**.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Restaurer une stratégie**.

   Remarque : la commande **Restaurer une stratégie** est également accessible depuis le menu **Actions**.

3. Sélectionnez le fichier XML à partir duquel la stratégie/le groupe de stratégies doit être restauré, puis cliquez sur **Ouvrir**.

La stratégie/le groupe de stratégie est restauré(e).

11.6 Attribution de stratégies

Pour attribuer des stratégies, vous avez besoin des droits d'**Accès complet** aux objets concernés.

1. Cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation, sélectionnez l'objet conteneur requis (par exemple, OU ou domaine).
3. Changez pour l'onglet **Stratégies**.

   Tous les éléments requis pour l'attribution de la stratégie sont affichés dans la zone d'action.

4. Pour attribuer une stratégie, faites-la glisser de la liste dans l'onglet **Stratégies**.
5. Vous pouvez définir une **Priorité** pour chaque stratégie en les organisant grâce au menu contextuel. Les paramètres des stratégies de niveau supérieur remplacent celles qui lui sont inférieures. Si vous sélectionnez **Ne pas remplacer** pour une stratégie, ses paramètres ne sont pas remplacés par ceux d'autres stratégies.

   Remarque : si vous sélectionnez **Ne pas remplacer** pour une stratégie de priorité inférieure, celle-ci acquiert une priorité plus élevée que celle d'une stratégie de niveau supérieur.

   Pour changer la **Priorité** ou le paramètre **Ne pas remplacer** pour des stratégies dans **Utilisateurs et ordinateurs**, vous avez besoin des droits d'**Accès complet** pour tous les objets auxquels les stratégies sont attribuées. Si vous n'avez pas les droits d'**Accès complet** pour tous les objets, les paramètres ne sont pas modifiables. Si vous essayez de modifier ces champs, une message d'information apparaît.

6. Les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation.

La stratégie s'applique à tous les groupes au sein de l'OU et/ou du domaine.

11.6.1 Activation des stratégies pour des groupes individuels

Les stratégies sont toujours attribuées à un OU, à un domaine ou à un groupe de travail. Elles s'appliquent par défaut à tous les groupes de ces objets conteneurs (les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation).

Toutefois, vous pouvez également définir des stratégies et les activer pour un ou plusieurs groupes. Ces stratégies s'appliquent ensuite exclusivement à ces groupes.

Remarque : pour activer les stratégies de groupes individuels, vous avez besoin des droits d'**Accès complet** pour le groupe concerné.

1. Attribuez la stratégie à l'OU contenant le groupe.
2. Les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation.
3. Faites glisser ces deux groupes de la zone d'activation jusqu'à la liste des **Groupes disponibles**. Dans cette constellation, la stratégie n'est efficace ni pour les utilisateurs ni pour les ordinateurs.
4. À présent, faites glisser le groupe requis (ou plusieurs groupes) de la liste des **Groupes disponibles** jusqu'à la zone d'activation.

Cette stratégie s'applique désormais exclusivement à ce groupe.

Si des stratégies ont également été attribuées à l'OU de niveau supérieur, cette stratégie s'applique à ce groupe en plus de celles définies pour l'OU tout entière.

11.7 Gestion des stratégies dans Utilisateurs et ordinateurs

À part la zone **Stratégies** dans le SafeGuard Management Center, vous pouvez aussi afficher et modifier le contenu d'une stratégie où l'attribution des stratégies est effectuée dans **Utilisateurs et ordinateurs**.

1. Cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'objet conteneur requis.
3. Vous pouvez ouvrir les stratégies pour les visualiser/modifier à partir de deux emplacements.
   - Passez sur l'onglet **Stratégies**, ou
   - passez sur l'onglet **RSOP**.
4. Cliquez avec le bouton droit de la souris sur la stratégie attribuée ou disponible requise et sélectionnez **Ouvrir** dans le menu contextuel.

   La boîte de dialogue des stratégies apparaît et vous pouvez visualiser et modifier les paramètres de stratégie.
5. Cliquez sur **OK** pour enregistrer vos changements.
6. Pour afficher les propriétés de stratégie, cliquez avec le bouton droit de la souris sur la stratégie et sélectionnez **Propriétés** dans le menu contextuel.

   La boîte de dialogue **Propriétés** de la stratégie apparaît. Ici, vous pouvez afficher les informations **Général** et **Attribution**.

11.8 Désactivation du déploiement de stratégies

En tant que responsable de la sécurité, vous pouvez désactiver le déploiement des ordinateurs d'extrémité. Pour ce faire, cliquez sur le bouton **Activer/désactiver le déploiement des stratégies** dans la barre d'outils du SafeGuard Management Center ou sélectionnez la commande **Activer/désactiver le déploiement des stratégies** dans le menu **Éditer**. Après désactivation du déploiement de stratégies, aucune stratégie n'est envoyée aux ordinateurs d'extrémité. Pour inverser la désactivation du déploiement de stratégies, cliquez sur le bouton ou sélectionnez de nouveau la commande.

Remarque : pour désactiver le déploiement de stratégies, un responsable de la sécurité doit disposer du droit "Activer/désactiver le déploiement des stratégies". Par défaut, ce droit a été affecté aux rôles prédéfinis de responsable principal de la sécurité et de responsable de la sécurité, mais il peut aussi être affecté à de nouveaux rôles définis par l'utilisateur.

11.9 Règles d'attribution et d'analyse des stratégies

La gestion et l'analyse des stratégies s'effectuent selon les règles décrites dans cette section.

11.9.1 Attribution et activation des stratégies

Pour activer une stratégie devant être mise en œuvre pour un utilisateur ou un ordinateur, vous devez d'abord l'attribuer à un objet conteneur (nœuds racine, domaine, OU, conteneur intégré ou groupe de travail). Pour que la stratégie attribuée à un utilisateur ou à un ordinateur devienne effective, lorsque vous attribuez une stratégie à un point quelconque de la hiérarchie, tous les ordinateurs (ordinateurs authentifiés) et tous les utilisateurs (utilisateurs authentifiés) sont activés automatiquement (l'attribution sans activation ne suffit pas). Tous les utilisateurs et tous les ordinateurs sont combinés dans ces groupes.

11.9.2 Héritage de stratégie

Les stratégies ne peuvent être transmises qu'entre objets conteneurs. Les stratégies peuvent être activées au sein d'un conteneur à supposer qu'il ne contienne aucun autre objet conteneur (au niveau du groupe). L'héritage entre groupes est impossible.

11.9.3 Hiérarchie d'héritage de stratégie

Lorsque des stratégies sont attribuées le long d'une chaîne hiérarchique, la stratégie la plus proche dans le cas d'un objet cible (utilisateur/ordinateur) a le niveau le plus élevé. Cela signifie que si la distance entre une stratégie et l'objet cible augmente, elle sera remplacée par toute autre stratégie plus proche.

11.9.4 Attribution directe des stratégies

L'utilisateur/ordinateur reçoit une stratégie attribuée directement à l'objet conteneur dans lequel il se trouve (l'appartenance d'un utilisateur de groupe placé dans un autre objet conteneur n'est pas suffisante). L'objet conteneur n'a pas hérité de cette stratégie !

11.9.5 Attribution indirecte des stratégies

L'utilisateur/ordinateur reçoit une stratégie que l'objet conteneur dans lequel il se trouve actuellement (l'appartenance en tant qu'utilisateur d'un groupe situé dans un autre objet conteneur n'est pas suffisante) a hérité d'un objet conteneur de niveau supérieur.

11.9.6 Activation/désactivation de stratégies

Pour qu'une stratégie soit effective pour un ordinateur/utilisateur, elle doit être activée au niveau du groupe (les stratégies peuvent uniquement être activées au niveau du groupe). Que ce groupe se trouve ou non dans le même objet conteneur n'a pas d'importance. Le seul point important est que l'utilisateur ou l'ordinateur ait été attribué directement ou indirectement (par héritage) à la stratégie.

Si un ordinateur ou un utilisateur se trouve en dehors d'une OU, ou d'une ligne d'héritage, et fait partie d'un groupe qui se trouve lui-même dans cette OU, cette activation ne s'applique **pas** à cet utilisateur/ordinateur. En effet, il n'existe pas d'attribution valide pour cet utilisateur ou cet ordinateur (directement ou indirectement). Le groupe était, en effet, activé mais une activation peut seulement s'appliquer aux utilisateurs et aux machines pour lesquels il existe aussi une attribution de stratégie. Ce qui signifie que l'activation des stratégies ne peut pas aller au-delà des limites de conteneur s'il n'y a pas d'attribution directe ou indirecte de la stratégie pour cet objet.

Une stratégie devient effective lorsqu'elle a été activée pour des groupes d'utilisateurs ou des groupes d'ordinateurs. Les groupes d'utilisateurs puis les groupes d'ordinateurs sont analysés (les utilisateurs authentifiés et les ordinateurs authentifiés sont également des groupes). Les deux résultats sont reliés par une instruction OR. Si ce lien OR donne une valeur positive pour la relation ordinateur/utilisateur, la stratégie s'applique.

Remarque : si plusieurs stratégies sont actives pour un objet, les stratégies individuelles sont groupées, en respectant néanmoins les règles décrites et fusionnées. Ce qui signifie que les paramètres réels d'un objet peuvent être composés de plusieurs stratégies différentes.

Un groupe peut avoir les paramètres d'activation suivants:

- Activé

  Une stratégie a été attribuée. Le groupe est affiché dans la zone d'activation du SafeGuard Management Center.

- Non activé

  Une stratégie a été attribuée. Le groupe ne se trouve pas dans la zone d'activation.

Si une stratégie est attribuée à un conteneur, le paramètre d'activation d'un groupe (activé) détermine si cette stratégie pour ce conteneur est incluse dans le calcul de la stratégie résultante.

Les stratégies héritées ne peuvent pas être contrôlées par ces activations. **Bloquer l'héritage de stratégie** doit être défini dans l'OU plus locale pour annuler l'effet de la stratégie globale à cet endroit.

11.9.7 Paramètres de l'utilisateur ou du groupe

Les paramètres de stratégie pour les utilisateurs (illustrés en **noir** dans le SafeGuard Management Center) sont prioritaires sur les paramètres de stratégie pour les ordinateurs (illustrés en **bleu** dans le SafeGuard Management Center). Si les paramètres de l'utilisateur sont spécifiés dans une stratégie pour les ordinateurs, ces paramètres seront remplacés par la stratégie pour l'utilisateur.

Remarque : seuls les paramètres de l'utilisateur sont remplacés. Si une stratégie pour les utilisateurs comporte également des paramètres machine (illustrés en **bleu**), ils ne sont pas remplacés par une stratégie d'utilisateur !

Exemple 1 :

Si une longueur de mot de passe de 4 a été définie pour un groupe d'ordinateurs, et si la valeur 3 du même paramètre a été définie pour le groupe d'utilisateurs, un mot de passe de longueur 3 s'applique à cet utilisateur sur un ordinateur appartenant à ce groupe d'ordinateurs.

Exemple 2 :

Si un intervalle de connexion au serveur de 1 minute est défini pour un groupe d'utilisateurs, et si la valeur 3 est définie pour un groupe de machines, la valeur 3 est utilisée car la valeur 1 minute est un paramètre machine ayant été défini dans une stratégie pour les utilisateurs.

11.9.8 Stratégies de chiffrement contradictoires

Deux stratégies, P1 et P2, sont créées. Le chiffrement basé sur fichier de l'unité E:\ a été défini pour P1, et le chiffrement basé sur volume de l'unité E:\ a été défini pour P2. P1 se voit attribuer l'OU **FBE-User** et P2 l'OU **VBE-User**.

Cas 1 : un utilisateur de l'OU **FBE-User** se connecte le premier au client W7-100 (ordinateur du conteneur). Le chiffrement de l'unité E:\ est basé sur le fichier. Si un utilisateur de l'OU **VBE-User** se connecte ensuite au client W7-100, le chiffrement de l'unité E:\ est basé sur le volume. Si les deux utilisateurs ont la même clé, tous deux peuvent accéder aux unités ou aux fichiers.

Cas 2 : un utilisateur de l'OU **VBE-User** se connecte le premier à l'ordinateur XP-100 (ordinateur du conteneur). Le lecteur est chiffré basé sur volume. Si, maintenant, un utilisateur de l'OU **FBE-User** se connecte et a la même clé que les utilisateurs de l'OU **VBE-User**, l'unité E:\ sera chiffré basé sur fichier dans la chiffrement basé sur volume (le chiffrement basé sur volume est conservé). Toutefois, si l'utilisateur de l'OU **FBE-User** n'a pas la même clé, il ne peut pas accéder à l'unité E:\.

11.9.9 Priorités au sein d'une attribution

Au sein d'une attribution, la stratégie ayant la plus haute priorité (1) se range au-dessus d'une stratégie ayant une priorité inférieure.

Remarque : si une stratégie ayant une priorité inférieure mais ayant été désignée **Ne pas remplacer** est attribuée au même niveau qu'une stratégie d'un niveau supérieur, cette stratégie sera prioritaire en dépit de son niveau inférieur.

11.9.10 Priorités au sein d'un groupe

Au sein d'un groupe, la stratégie ayant la plus haute priorité (1) se range au-dessus d'une stratégie ayant une priorité inférieure.

11.9.11 Indicateurs d'état

La définition d'indicateurs d'état permet de changer les règles par défaut pour les stratégies.

- **Bloquer l'héritage de stratégie**

  Paramètre des conteneurs pour lesquels vous ne souhaitez pas que des stratégies de niveau supérieur s'appliquent (cliquez avec le bouton droit sur l'objet dans la fenêtre de navigation Propriétés).

  Si vous ne souhaitez pas qu'un objet conteneur hérite d'une stratégie d'un objet plus élevé, sélectionnez **Bloquer l'héritage de stratégie** pour l'en empêcher. Si **Bloquer l'héritage de stratégie** a été sélectionné pour un objet conteneur, il ne sera pas affecté par les paramètres d'une stratégie d'un niveau supérieur (exception : **Ne pas remplacer** activé lorsqu'une stratégie a été attribuée).

- **Ne pas remplacer**

  Définie au cours de l'attribution, cette stratégie ne peut pas être remplacée par une autre.

  Plus l'attribution de la stratégie **Ne pas remplacer** est éloignée de l'objet cible, plus cette stratégie a d'effet sur tous les objets conteneurs de niveau inférieur. Cela signifie qu'un conteneur de niveau supérieur soumis à **Ne pas remplacer** remplace les paramètres de stratégie d'un conteneur de niveau inférieur. Il est donc, par exemple, possible de définir une stratégie de domaine dont les paramètres ne peuvent pas être remplacés, même si **Bloquer l'héritage de stratégie** a été défini pour une OU.

  Remarque : si une stratégie ayant une priorité inférieure mais ayant été désignée **Ne pas remplacer** est attribuée au même niveau qu'une stratégie d'un niveau supérieur, cette stratégie sera prioritaire en dépit de son niveau inférieur.

11.9.12 Paramètres dans les stratégies

11.9.12.1 Paramètres de relecture de la machine

Vous pouvez trouver ce paramètre sous :

Éléments de stratégie > stratégie du type **Paramètres généraux** > **Chargement de paramètres** > **Mode de récursivité des stratégies**.

Si vous sélectionnez **Paramètres machine de relecture** dans le champ **Mode de récursivité des stratégies** d'une stratégie du type **Paramètres généraux** et que la stratégie provient d'un ordinateur (**Paramètres machine de relecture** n'affecte pas les stratégies utilisateur), cette stratégie est relue à la fin de l'analyse. Ceci remplace ensuite les paramètres de l'utilisateur et les paramètres de la machine s'appliquent. Tous les paramètres de la machine hérités directement ou indirectement par la machine (y compris les stratégies qui n'ont pas été

appliquées par le mode de récursivité des stratégies **Paramètres machine de relecture**) sont remplacés.

11.9.12.2 Ignorer l'utilisateur

Vous pouvez trouver ce paramètre sous :

Éléments de stratégie > stratégie du type **Paramètres généraux** > **Chargement de paramètres** > **Mode de récursivité des stratégies**.

Si vous sélectionnez **Ignorer l'utilisateur** pour une stratégie d'ordinateur dans le champ **Mode de récursivité des stratégies** d'une stratégie du type **Paramètres généraux** et si la stratégie provient d'une machine, seuls les paramètres de la machine sont analysés. Les paramètres de l'utilisateur ne sont pas analysés.

11.9.12.3 Aucun bouclage

Vous pouvez trouver ce paramètre sous :

Éléments de stratégie > stratégie du type **Paramètres généraux** > **Chargement de paramètres** > **Mode de récursivité des stratégies**.

Aucun blocage décrit le comportement standard. Les stratégies de l'utilisateur sont prioritaires sur celles de l'ordinateur.

11.9.12.4 Analyse des paramètres « Ignorer l'utilisateur » et « Paramètres machine de relecture »

S'il existe des attributions de stratégies actives, les stratégies de la machine sont analysées et regroupées d'abord. Si, avec le **Mode de récursivité des stratégies**, ce regroupement de stratégies individuelles aboutit à la valeur **Ignorer l'utilisateur**, les stratégies définies pour l'utilisateur ne sont pas analysées. Cela signifie que les mêmes stratégies s'appliquent à la fois pour l'utilisateur et pour la machine.

Si, après regroupement des stratégies individuelles, la valeur avec l'attribut **Mode de récursivité des stratégies** est **Paramètres de relecture de la machine**, les stratégies de l'utilisateur sont combinées à celles de la machine. Après le regroupement, les stratégies de la machine sont réécrites et, le cas échéant, remplacent les paramètres de stratégie de l'utilisateur. Si un paramètre est présent dans les deux stratégies, la valeur de la stratégie de la machine remplace celle de la stratégie de l'utilisateur.

Si le regroupement des stratégies individuelles de la machine produit la valeur par défaut (**Pas de mode de récursivité des stratégies**), les paramètres de l'utilisateur sont prioritaires par rapport à ceux de la machine.

11.9.12.5 Ordre d'exécution des stratégies

Ignorer l'utilisateur Ordinateurs

Paramètres machine de relecture Ordinateur -> Utilisateur -> Ordinateur. La première "exécution sur machine" est requise pour les stratégies qui sont écrites avant que la connexion utilisateur n'intervienne (par exemple, image d'arrière-plan lors de la connexion).

Aucun bouclage (paramètre standard) : Ordinateur -> Utilisateur

11.9.13 Autres définitions

C'est l'origine d'une stratégie qui permet de déterminer s'il s'agit d'une stratégie d'utilisateur ou d'une stratégie de machine. Un objet de l'utilisateur "appelle" une stratégie d'utilisateur, et un ordinateur "appelle" une stratégie d'ordinateur. La même stratégie peut être une stratégie de machine ou d'utilisateur, selon le point de vue.

- **Stratégie d'utilisateur**

  Toute stratégie fournie par l'utilisateur pour l'analyse. Si une stratégie est mise en œuvre via un seul utilisateur, les paramètres associés à la machine de cette stratégie ne sont pas appliqués, en d'autres termes, les paramètres associés à l'ordinateur ne s'appliquent pas. Les valeurs par défaut s'appliquent.

- **Stratégie d'ordinateur**

  Toute stratégie fournie par la machine pour l'analyse. Si une stratégie est mise en œuvre via un seul ordinateur, les paramètres spécifiques à l'utilisateur pour cette stratégie sont également appliqués ! La stratégie de l'ordinateur représente par conséquent une stratégie « pour tous les utilisateurs ».

12 Utilisation des packages de configuration

Dans SafeGuard Management Center, vous pouvez créer les types de packages de configuration suivants :

- **Package de configuration pour ordinateurs d'extrémité administrés**

  Les ordinateurs d'extrémité connectés au serveur SafeGuard Enterprise reçoivent leurs stratégies par le biais de ce serveur. Pour garantir un bon fonctionnement une fois le logiciel client SafeGuard Enterprise installé, vous devez créer un package de configuration pour les ordinateurs administrés et le déployer sur ceux-ci.

  Une fois la première configuration de l'ordinateur d'extrémité effectuée par le package de configuration, l'ordinateur reçoit des stratégies par le biais du serveur SafeGuard Enterprise après que vous avez attribué celles-ci dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center.

- **Package de configuration pour ordinateurs d'extrémité non administrés**

  Les ordinateurs d'extrémité non administrés ne sont connectés au serveur SafeGuard Enterprise à aucun moment, et fonctionnent en mode autonome. Ces ordinateurs reçoivent leurs stratégies par packages de configuration. Pour garantir un bon fonctionnement, vous devez créer un package de configuration contenant les groupes de stratégies appropriés, puis le distribuer sur les ordinateurs d'extrémité à l'aide des mécanismes de distribution de l'entreprise. À chaque fois que vous modifiez des paramètres de stratégie, vous devez créer de nouveaux packages de configuration et les distribuer sur les ordinateurs d'extrémité.

  Remarque : les packages de configuration pour ordinateurs d'extrémité non administrés peuvent uniquement être utilisés sur les ordinateurs d'extrémité Windows.

- **Package de configuration pour le serveur SafeGuard Enterprise**

  Pour garantir un bon fonctionnement, vous devez créer un package de configuration pour le serveur SafeGuard Enterprise qui définira la base de données et la connexion SSL, activera l'API de script, etc.

- **Package de configuration pour les Mac**

  Les ordinateurs Macs reçoivent l'adresse du serveur et le certificat d'entreprise par le biais de ce package. Ils envoient les informations sur leur état qui sont ensuite affichées dans le SafeGuard Management Center. Retrouvez plus d'informations sur la création des packages de configuration pour Macs à la section Création d'un package de configuration pour Macs à la page 277.

Remarque : vérifiez votre réseau et vos ordinateurs à intervalles réguliers pour détecter les packages de configuration obsolètes ou non utilisés. De même, pour des raisons de sécurité, n'oubliez pas de les supprimer. Assurez-vous de toujours désinstaller les anciens packages de configuration avant d'installer tout nouveau package de configuration sur l'ordinateur/le serveur.

12.1 Création d'un package de configuration pour les ordinateurs administrés

Conditions préalables

- Dans la zone de navigation **Utilisateurs et ordinateurs**, sous l'onglet **Inventaire**, vérifiez si une modification d'un certificat d'entreprise est nécessaire pour les ordinateurs d'extrémité qui doivent recevoir le nouveau package de configuration. Si le champ **Certificat d'entreprise actuel** n'est pas sélectionné, les certificats d'entreprise actuellement actifs dans la base de données SafeGuard Enterprise et sur l'ordinateur diffèrent et une modification de certificat d'entreprise est donc requise.

1. Dans le SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Attribuez un serveur SafeGuard Enterprise principal (le serveur secondaire n'est pas nécessaire).
6. Si besoin est, indiquez un groupe de stratégies, créé auparavant dans le SafeGuard Management Center, qui sera appliqué aux ordinateurs d'extrémité. Si vous voulez utiliser des comptes de service utilisateur pour les tâches postérieures à l'installation sur l'ordinateur d'extrémité, assurez-vous d'inclure le paramètre de stratégie respectif dans ce premier groupe de stratégie. Retrouvez plus d'informations à la section Listes de comptes de service pour la connexion à Windows à la page 99.
7. Si le certificat d'entreprise actuellement actif dans la base de données SafeGuard Enterprise diffère de celui présent sur les ordinateurs d'extrémité qui doivent recevoir le nouveau package de configuration, sélectionnez le **CCO** (Company Certificate Change Order) adéquat. Dans **Utilisateurs et ordinateurs**, dans l'onglet **Inventaire** du domaine approprié, de l'OU ou de l'ordinateur, une coche manquante sous **Certificat d'entreprise actuel** indique qu'une modification de certificat d'entreprise est nécessaire. Les informations sont disponibles sur le CCO requis dans l'onglet **CCO** de l'**Outil du package de configuration** dans le menu **Outils**.

   Remarque : si les certificats d'entreprise actuellement actifs dans la base de données SafeGuard Enterprise et sur l'ordinateur d'extrémité ne correspondent pas et si aucun **CCO** approprié n'est inclus, le déploiement du nouveau package de configuration sur l'ordinateur d'extrémité échouera.

8. Sélectionnez le mode **Chiffrement du transport** définissant comment chiffrer la connexion entre le client SafeGuard Enterprise et le serveur SafeGuard Enterprise : chiffrement Sophos ou SSL.

   Le protocole SSL présente l'avantage d'être standard et de permettre d'établir une connexion plus rapidement qu'en utilisant le chiffrement de transport SafeGuard. Le chiffrement SSL est sélectionné par défaut. Retrouvez plus d'informations sur la sécurisation des connexions de transport avec SSL dans le *Guide d'installation de SafeGuard Enterprise*.

9. Indiquez un chemin de sortie pour le package de configuration (MSI).

10. Cliquez sur **Créer un package de configuration**.

    Si vous avez sélectionnez le chiffrement SSL en tant que mode de **Chiffrement du transport**, la connexion au serveur est validée. En cas d'échec de la connexion, un message d'avertissement s'affiche.

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer ce package aux ordinateurs d'extrémité et le déployer sur ceux-ci.

12.2 Création d'un package de configuration pour les ordinateurs non administrés

1. Dans le menu **Outils** du SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client autonome**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Indiquez un **Groupe de stratégies** préalablement créé dans SafeGuard Management Center et que vous souhaitez appliquer aux ordinateurs d'extrémité.
6. Sous **Emplacement de la sauvegarde de la clé**, indiquez ou sélectionnez un chemin réseau partagé pour le stockage du fichier de récupération de clé. Saisissez le chemin de partage sous la forme suivante : **`\\ordinateur réseau\`**, par exemple **`\\monentreprise.edu\`**. Si vous n'indiquez pas de chemin ici, l'utilisateur final sera invité à indiquer l'emplacement de stockage de ce fichier lors de sa première connexion à l'ordinateur d'extrémité, suite à l'installation.

   Le fichier de récupération de clé (XML) est requis pour activer la récupération des ordinateurs protégés par Sophos SafeGuard. Il est généré sur chaque ordinateur protégé par Sophos SafeGuard.

   Remarque : assurez-vous d'enregistrer ce fichier de récupération de clé à un emplacement de fichier accessible pour le support. Les fichiers peuvent également être fournis au support à l'aide de différents mécanismes. Ce fichier est chiffré par le certificat d'entreprise. Il peut donc être enregistré sur un support externe ou sur le réseau pour être fourni au support technique à des fins de récupération. Il peut également être envoyé par e-mail.

7. Sous **Groupe d'authentification au démarrage**, vous pouvez sélectionner le groupe d'utilisateurs de l'authentification au démarrage à attribuer à l'ordinateur d'extrémité. Les utilisateurs de l'authentification au démarrage peuvent accéder à l'ordinateur d'extrémité pour des tâches administratives après activation de l'authentification au démarrage SafeGuard. Pour attribuer des utilisateurs de l'authentification au démarrage, le groupe d'authentification au démarrage doit avoir été préalablement créé dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center.
8. Indiquez un chemin de sortie pour le package de configuration (MSI).
9. Cliquez sur **Créer un package de configuration**.

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer ce package aux ordinateurs d'extrémité et le déployer sur ceux-ci.

12.3 Création d'un package de configuration pour les Macs

Un package de configuration pour un Mac contient les informations sur le serveur et le certificat d'entreprise. Le Mac utilise ces informations pour signaler les informations d'état (authentification au démarrage SafeGuard active/inactive, état de chiffrement,...). Les informations d'état apparaissent dans SafeGuard Management Center.

1. Dans le menu **Outils** du SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Attribuez un serveur SafeGuard Enterprise principal (le serveur secondaire n'est pas nécessaire).
6. Sélectionnez **SSL** comme **Chiffrement du transport** pour la connexion entre l'ordinateur d'extrémité et le serveur SafeGuard Enterprise. **Sophos** en tant que **Chiffrement de transport** n'est pas pris en charge pour Mac.
7. Indiquez un chemin de sortie pour le package de configuration (ZIP).
8. Cliquez sur **Créer un package de configuration**.

   La connexion au serveur pour le mode **Chiffrement du transport** SSL est validé. En cas d'échec de la connexion, un message d'avertissement s'affiche.

Le package de configuration (ZIP) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer ce package sur vos Macs et le déployer sur ceux-ci. Retrouvez plus d'informations dans les manuels de *Sophos SafeGuard Disc encryption pour Mac* et de *Sophos SafeGuard File Encryption pour Mac*.

13 Authentification au démarrage de SafeGuard

Remarque : cette description concerne les ordinateurs d'extrémité Windows 7 sur lesquels est installé le chiffrement intégral du disque SafeGuard. Retrouvez plus d'informations sur les méthodes de connexion pour les ordinateurs d'extrémité Windows 7 et Windows 8 avec le Chiffrement de lecteur BitLocker dans la documentation Microsoft.

SafeGuard Enterprise identifie l'utilisateur avant même le démarrage du système d'exploitation. Pour ce faire, le noyau du système de SafeGuard Enterprise démarre en amont. Il est protégé contre toute modification puis il est enregistré et masqué sur le disque dur. Lorsque l'utilisateur est correctement authentifié dans l'authentification au démarrage SafeGuard, seul le système d'exploitation effectif (Windows) est lancé depuis la partition chiffrée. L'utilisateur est connecté automatiquement à Windows. La procédure est identique lorsque l'ordinateur est sorti du mode veille prolongée.



L'authentification au démarrage SafeGuard offre :

- Une interface utilisateur graphique, avec prise en charge de la souris et des fenêtres pouvant être déplacées, pour plus de facilité et de lisibilité ;
- Une présentation graphique qui, en suivant les instructions, peut être personnalisée pour les ordinateurs d'entreprise (image d'arrière-plan, image de connexion, message d'accueil, etc.) ;
- La prise en charge de nombreux lecteurs de cartes et d'un grand nombre de cartes à puce ;
- La prise en charge des comptes utilisateur Windows et des mots de passe dès l'étape de préinitialisation, ce qui évite à l'utilisateur de devoir mémoriser des informations d'identification distinctes ;
- La prise en charge du format Unicode et par conséquent des mots de passe et des interfaces utilisateur en langue étrangère.

13.1 Connexion

SafeGuard Enterprise fonctionne avec la connexion basée sur certificat. Les utilisateurs ont besoin de clés et de certificats pour se connecter lors de l'authentification au démarrage

SafeGuard. La clé et les certificats spécifiques à un utilisateur ne sont cependant créés qu'après une connexion Windows. Seuls les utilisateurs connectés à Windows peuvent être authentifiés à partir de l'authentification au démarrage SafeGuard.

Pour clarifier la manière dont un utilisateur se connecte à SafeGuard Enterprise, vous trouverez ci-après une brève introduction. Retrouvez une description détaillée des procédures de connexion d'authentification au démarrage SafeGuard dans le *Manuel d'utilisation de SafeGuard Enterprise*.

Connexion automatique de SafeGuard

Lors de la première connexion, la connexion automatique à SafeGuard Enterprise s'affiche après le démarrage de l'ordinateur d'extrémité.

Que se passe-t-il ?

1. Un utilisateur est connecté automatiquement.
2. Le client est enregistré automatiquement sur le serveur SafeGuard Enterprise.
3. La clé machine est envoyée au serveur SafeGuard Enterprise et stockée dans la base de données SafeGuard Enterprise.
4. Les stratégies de la machine sont envoyées à l'ordinateur d'extrémité.

Connexion Windows

La boîte de dialogue de connexion de Windows s'affiche. L'utilisateur se connecte.

Que se passe-t-il ?

1. L'identifiant utilisateur et un hachage des codes d'accès de l'utilisateur sont envoyés au serveur.
2. Les stratégies, certificats et clés utilisateur sont créés et envoyés à l'ordinateur d'extrémité.
3. L'authentification au démarrage SafeGuard est activée.

Connexion à l'authentification au démarrage SafeGuard

Lorsque le client redémarre, l'authentification au démarrage SafeGuard apparaît.

Que se passe-t-il ?

1. L'utilisateur a les certificats et les clés à disposition et il peut se connecter lors de l'authentification au démarrage SafeGuard.
2. Toutes les données sont chiffrées et sécurisées avec la clé publique RSA de l'utilisateur.
3. Tous les autres utilisateurs qui souhaitent se connecter doivent, au préalable, être importés dans l'authentification au démarrage SafeGuard.

13.1.1 Retard de connexion

Sur un ordinateur protégé par SafeGuard Enterprise, un délai de connexion s’applique si un utilisateur fournit des codes d'accès incorrects pendant l’authentification à Windows ou à l'authentification au démarrage SafeGuard. Le retard de connexion augmente à chaque échec de tentative de connexion. Après un échec de connexion, une boîte de dialogue apparaît et affiche le délai restant.

Remarque : si un utilisateur saisit un code PIN incorrect lors de la connexion sur la carte à puce, il n'y a aucun retard de connexion.

Vous pouvez indiquer le nombre de tentatives de connexion autorisées dans une stratégie du type **Authentification** en vous aidant pour cela de l'option **Nbre maximum d'échecs de connexion**. Lorsque le nombre maximum d'échecs de tentative de connexion est atteint, l'ordinateur est verrouillé. Pour déverrouiller leurs ordinateurs, les utilisateurs doivent lancer une procédure Challenge/Réponse.

13.2 Enregistrement d'utilisateurs SafeGuard Enterprise supplémentaires

Le premier utilisateur à se connecter à Windows est enregistré automatiquement dans l'authentification au démarrage SafeGuard. Au départ, aucun autre utilisateur Windows ne peut se connecter à l'authentification au démarrage SafeGuard.

Les autres utilisateurs doivent être importés avec l'aide du premier. Retrouvez une description détaillée de l'importation d'autres utilisateurs, dans le Manuel d'utilisation de SafeGuard Enterprise.

Un paramètre de stratégie spécifie qui est autorisé à importer un nouvel utilisateur. Vous pouvez trouver cette stratégie dans SafeGuard Management Center sous

Éléments de stratégie

- Type : **Paramètres de machine spécifiques**
- Champ : **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour**

Paramètre par défaut : **Propriétaire**

Le propriétaire d'un ordinateur d'extrémité est spécifié dans SafeGuard Management Center sous

Utilisateurs et ordinateurs

- Sélectionnez <nom de l'ordinateur d'extrémité>.
- Onglet **Utilisateurs**

Remarque : safeguard Enterprise propose des utilisateurs de l'authentification au démarrage (comptes locaux prédéfinis) qui permettent aux utilisateurs de se connecter (connexion à l'authentification au démarrage SafeGuard) à des ordinateurs d'extrémité, une fois l'authentification au démarrage SafeGuard activée, pour effectuer des tâches administratives. Les comptes sont définis dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center (identifiant utilisateur et mot de passe) et attribués aux ordinateurs d'extrémité dans les groupes d'authentification au démarrage. Retrouvez plus d'informations à la section Utilisateurs de l'authentification au démarrage pour connexion à l'authentification au démarrage SafeGuard à la page 104.

13.3 Configuration de l'authentification au démarrage SafeGuard

La boîte de dialogue de l'authentification au démarrage SafeGuard comporte les composants suivants :

- Image de connexion
- Texte des boîtes de dialogue
- Langue de la disposition du clavier



Vous pouvez modifier l'apparence de la boîte de dialogue de l'authentification au démarrage SafeGuard selon vos préférences à l'aide des paramètres de stratégie du SafeGuard Management Center.

13.3.1 Image d'arrière-plan et de connexion

Par défaut, les images d'arrière-plan et de connexion qui s'affichent dans l'authentification au démarrage SafeGuard sont conçues selon SafeGuard. Vous pouvez changer ces images pour afficher, par exemple, un logo d'entreprise.

Les images d'arrière-plan et de connexion sont définies dans une stratégie du type **Paramètres généraux**.

Utilisées dans SafeGuard Enterprise, les images d'arrière-plan et de connexion doivent respecter certaines conditions :

Image d'arrière-plan

Taille de fichier maximale pour toutes les images d'arrière-plan : **500 Ko**

SafeGuard Enterprise prend en charge deux variantes d'images d'arrière-plan:

- **1024 x 768** (mode VESA)

  Couleurs : aucune restriction

  Stratégie du type **Paramètres généraux**, option **Image d'arrière-plan dans l'authentification au démarrage (basse résolution)**

- **640 x 480** (mode VGA)

Couleurs : 16

Stratégie du type **Paramètres généraux**, option **Image d'arrière-plan dans l'authentification au démarrage (basse résolution)**

Image de connexion

Taille de fichier maximale pour toutes les images de connexion : **100 Ko**

SafeGuard Enterprise prend en charge deux variantes d'images de connexion :

- **413 x 140**

  Couleurs : aucune restriction

  Stratégie du type **Paramètres généraux**, option **Image de connexion dans la POA**

- **413 x 140**

  Couleurs : 16

  Stratégie du type **Paramètres généraux**, option **Image de connexion dans l'authentification au démarrage (basse résolution)**

Les images doivent être créés en premier sous la forme de fichiers (fichiers BMP, PNG, JPG), puis enregistrés dans la fenêtre de navigation.

13.3.1.1 Enregistrement d'images

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Images** et sélectionnez **Nouveau** > **Image**.
2. Entrez le nom de l'image dans le champ **Nom de l'image**.
3. Cliquez sur **[...]** pour sélectionner l'image préalablement créée.
4. Cliquez sur **OK**.

La nouvelle image apparaît sous la forme d'un nœud secondaire de **Images** dans la zone de navigation de stratégie. Si vous sélectionnez l'image, elle s'affiche dans la zone d'action. L'image peut désormais être sélectionnée lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres images. Toutes les images enregistrées s'affichent sous la forme de nœuds secondaires.

Remarque : vous pouvez utiliser le bouton **Modifier l'image** pour changer l'image attribuée.

13.3.2 Texte d'informations défini par l'utilisateur dans l'authentification au démarrage SafeGuard

Vous pouvez personnaliser l'authentification au démarrage SafeGuard en affichant les **textes d'informations définis par l'utilisateur** :

- Texte d'informations affiché lors du lancement d'une procédure Challenge/Réponse pour la récupération de connexion (par exemple : “Contactez le bureau de support en appelant au 01234-56789.”)

  Vous pouvez définir un texte d'informations en utilisant l'option **Texte d'informations** dans une stratégie de type **Paramètres généraux**

- Mentions légales affichées après la connexion à l'authentification au démarrage SafeGuard

  Vous pouvez définir un texte de mention légale en utilisant l'option **Texte de la mention légale** dans la stratégie de type **Paramètres de machine spécifiques**

- Texte d'informations supplémentaires affiché après la connexion à l'authentification au démarrage SafeGuard

  Vous pouvez définir un texte d'informations supplémentaires en utilisant l'option **Texte d'informations supplémentaires** dans la stratégie de type **Paramètres de machine spécifiques**

13.3.2.1 Enregistrement des textes d'informations

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans le SafeGuard Management Center. La taille maximale des fichiers de textes d'informations est de **50 Ko**. SafeGuard Enterprise utilise les textes codés en Unicode UTF-16 uniquement. Si vous ne créez pas les fichiers texte dans ce format, ils seront automatiquement convertis lorsqu'ils seront enregistrés. Les caractères spéciaux doivent par conséquent être utilisés avec prudence dans les textes d'informations créés pour l'authentification au démarrage SafeGuard. Il est possible que certains de ces caractères n'apparaissent pas correctement.

Pour enregistrer des textes d'informations :

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau** > **Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque : vous pouvez utiliser le bouton **Modifier le texte** pour ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

13.3.3 Langue de la boîte de dialogue d'authentification au démarrage SafeGuard

Après l'installation du logiciel de chiffrement SafeGuard Enterprise, le texte de la boîte de dialogue de l'authentification au démarrage SafeGuard est affiché dans la langue par défaut définie dans les Options régionales et linguistiques de Windows sur l'ordinateur d'extrémité, lors de l'installation de SafeGuard Enterprise.

Vous pouvez changer la langue du texte de la boîte de dialogue de l'authentification au démarrage SafeGuard après l'installation de SafeGuard Enterprise à l'aide de l'une des deux méthodes suivantes :

- Changez la langue par défaut dans les Options régionales et linguistiques Windows sur l'ordinateur d'extrémité. Après deux redémarrages de l'ordinateur par l'utilisateur, le nouveau paramètre de langue est actif dans l'authentification au démarrage SafeGuard.
- Créez une stratégie du type **Paramètres généraux**, choisissez la langue dans le champ **Langue utilisée sur le client** et déployez la stratégie sur l'ordinateur d'extrémité.

Remarque : si vous définissez une stratégie et la déployez sur l'ordinateur d'extrémité, la langue choisie dans la stratégie s'applique au lieu de celle indiquée dans les Options régionales et linguistiques de Windows.

13.3.4 Disposition du clavier

Chaque pays ou presque a une disposition de clavier qui lui est propre. La disposition du clavier dans l'authentification au démarrage SafeGuard est importante lorsque vous saisissez des noms d'utilisateur, des mots de passe et des codes de réponse.

Par défaut, SafeGuard Enterprise adopte la disposition de clavier de l'authentification au démarrage SafeGuard qui a été définie dans les Options régionales et linguistiques de Windows pour l'utilisateur Windows par défaut au moment où SafeGuard Enterprise a été installé. Si « Allemand » est la disposition de clavier définie sous Windows, la disposition allemande du clavier sera utilisée dans l'authentification au démarrage SafeGuard.

La langue de la disposition du clavier utilisée est affichée dans l'authentification au démarrage SafeGuard (par exemple "FR" pour français). Outre la disposition du clavier par défaut, la disposition du clavier américain (anglais) peut également être utilisée.

Il existe un certain nombre d'exceptions :

- La disposition du clavier est effectivement prise en charge, mais l'absence d'une police de caractères (par exemple, pour le bulgare) signifie que seuls les caractères spéciaux sont affichés dans le champ **Nom d'utilisateur**.
- Aucune disposition du clavier n'est disponible (par exemple, pour la République Dominicaine). Dans ces situations, l'authentification au démarrage SafeGuard revient à la disposition du clavier d'origine. Pour la République Dominicaine, il s'agit de l'"Espagnol".
- Lorsque le nom d'utilisateur et le mot de passe comportent des caractères non reconnus par la disposition du clavier choisie ou par celle de secours, l'utilisateur ne peut pas se connecter à l'authentification au démarrage SafeGuard.

Remarque : toutes les dispositions du clavier non prises en charge utilisent la disposition de clavier américaine par défaut. Cela signifie également que les seuls caractères reconnus et pouvant être saisis au clavier sont ceux pris en charge dans la disposition du clavier américain. De la sorte, les utilisateurs peuvent uniquement se connecter lors de l'authentification au démarrage SafeGuard si leur nom d'utilisateur et leur mot de passe sont composés de caractères pris en charge dans la disposition du clavier de la langue correspondante.

Clavier virtuel

SafeGuard Enterprise propose aux utilisateurs un clavier virtuel qu'ils peuvent afficher/masquer à l'authentification au démarrage SafeGuard et qui leur permet d'utiliser les touches tactiles pour saisir des codes d'accès.

En tant que responsable de la sécurité, vous pouvez activer/désactiver l'affichage du clavier virtuel à l'aide d'une stratégie du type **Paramètres de machine spécifiques** avec l'option **Clavier virtuel en POA**.

La prise en charge du clavier virtuel doit être activée/désactivée par un paramètre de stratégie.

Le clavier virtuel accepte différentes dispositions et il est possible de changer la disposition à l'aide des mêmes options que pour la disposition du clavier de l'authentification au démarrage SafeGuard.

13.3.4.1 Modification de la disposition du clavier

La disposition du clavier pour l'authentification au démarrage SafeGuard, clavier virtuel inclus, peut être modifiée rétrospectivement.

1. Sélectionnez **Démarrer** > **Panneau de configuration** > **Options régionales et linguistiques** > **Options avancées**.
2. Dans l'onglet **Options régionales**, sélectionnez la langue souhaitée.
3. Dans l'onglet **Options avancées**, sélectionnez **Appliquer tous les paramètres au compte d'utilisateur actuel et au profil utilisateur par défaut** sous **Paramètres par défaut du compte d'utilisateur**.
4. Cliquez sur **OK**.

L'authentification au démarrage SafeGuard garde en mémoire la disposition du clavier utilisée au cours de la dernière connexion et l'active automatiquement à la connexion suivante. Cette opération nécessite que vous redémarriez l'ordinateur d'extrémité deux fois. Si la disposition du clavier mémorisée est désactivée dans les **Options régionales et linguistiques**, elle est tout de même utilisée jusqu'à ce que l'utilisateur en sélectionne une autre.

Remarque : vous devez modifier la langue de la disposition du clavier pour les programmes autres que Unicode.

Si la langue souhaitée n'est pas disponible sur l'ordinateur, Windows peut vous inviter à l'installer. Après avoir effectué cette opération, vous devez redémarrer l'ordinateur deux fois pour que l'authentification au démarrage SafeGuard puisse lire la nouvelle disposition du clavier et la définir.

Vous pouvez changer la disposition du clavier requise pour l'authentification au démarrage SafeGuard à l'aide de la souris ou du clavier (**Alt+Maj**).

Pour voir les langues installées et disponibles sur le système, sélectionnez **`Démarrer > Exécuter > regedit > HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`**.

13.4 Raccourcis clavier pris en charge dans l'authentification au démarrage SafeGuard

Certains paramètres et fonctionnalités du matériel peuvent générer des problèmes lors du démarrage des ordinateurs et provoquer le blocage du système. L'authentification au démarrage SafeGuard prend en charge plusieurs raccourcis clavier pour modifier les paramètres matériels et désactiver les fonctionnalités. De plus, des listes « grises » et « noires » contenant les fonctions connues pour provoquer des problèmes sont intégrées au fichier .msi installé sur l'ordinateur.

Nous vous recommandons d'installer une version mise à jour du fichier de configuration de l'authentification au démarrage SafeGuard avant de procéder au déploiement de SafeGuard Enterprise. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : http://www.sophos.com/fr-fr/support/knowledgebase/65700.aspx.

Vous pouvez personnaliser ce fichier pour qu'il reflète le matériel d'un environnement spécifique.

Remarque : lorsqu'un fichier personnalisé est utilisé, celui-ci remplace le fichier intégré au fichier .msi. Le fichier par défaut s'applique uniquement lorsqu'aucun fichier de configuration de l'authentification au démarrage SafeGuard n'est défini ou trouvé.

Pour installer le fichier de configuration de l'authentification au démarrage SafeGuard, saisissez la commande suivante :

```
MSIEXEC /i <package MSI client> POACFG=<chemin du fichier de
configuration de l'authentification au démarrage SafeGuard>
```

Vous pouvez nous aider à améliorer la compatibilité en exécutant un outil que nous vous fournissons pour recueillir seulement les informations matérielles correspondantes. L'outil est très simple à utiliser. Les informations recueillies sont ajoutées au fichier de configuration matérielle.

Pour plus d'informations, consultez l'article http://www.sophos.com/fr-fr/support/knowledgebase/110285.aspx.

Les raccourcis clavier suivants sont pris en charge dans l'authentification au démarrage SafeGuard :

- **Maj F3** = prise en charge héritée USB (actif/inactif)
- **Maj F4** = mode graphique VESA (actif/inactif)
- **Maj F5** = prise en charge USB 1.x et 2.0 (actif/inactif)
- **Maj F6** = contrôleur ATA (actif/inactif)
- **Maj F7** = prise en charge USB 2.0 seulement (actif/inactif)

  La prise en charge USB 1.x reste tel que définie par Maj F5.
- **Maj F9** = ACPI/APIC (actif/inactif)

Matrice de dépendance des raccourcis clavier USB

Maj F3	Maj F5	Maj F7	Hérité	USB 1.x	USB 2.0	Commentaire
désactivé	désactivé	désactivé	activé	activé	activé	3.
activé	désactivé	désactivé	désactivé	activé	activé	Par défaut
désactivé	activé	désactivé	activé	désactivé	désactivé	1., 2.
activé	activé	désactivé	activé	désactivé	désactivé	1., 2.
désactivé	désactivé	activé	activé	activé	désactivé	3.
activé	désactivé	activé	désactivé	activé	désactivé	
désactivé	activé	activé	activé	désactivé	désactivé	
activé	activé	activé	activé	désactivé	désactivé	2.

1. Maj F5 désactive USB 1.x et USB 2.0.

   Remarque : si vous appuyez sur Maj - F5 pendant le démarrage, vous réduirez considérablement la durée du lancement de l'authentification au démarrage SafeGuard. Sachez cependant que si l'ordinateur est équipé d'un clavier USB ou d'une souris USB, ces derniers peuvent être désactivés si vous appuyez sur **Maj F5**.

2. Si aucun support USB n'est actif, l'authentification au démarrage SafeGuard tente d'utiliser BIOS SMM au lieu de sauvegarder et de restaurer le contrôleur USB. Le mode hérité peut fonctionner dans ce scénario.
3. Le support hérité est actif, USB est actif. L'authentification au démarrage SafeGuard tente de sauvegarder et de restaurer le contrôleur USB. Il se peut que le système se bloque selon la version du BIOS utilisée.

Vous pouvez spécifier les modifications pouvant être effectuées en utilisant des raccourcis clavier lors de l'installation du logiciel de chiffrement SafeGuard Enterprise à l'aide d'un fichier .mst. Pour ce faire, utilisez l'appel approprié en combinaison avec msiexec.

NOVESA	Définit si le mode VESA ou VGA est utilisé.0 = mode VESA (standard)1 = mode VGA
NOLEGACY	Définit si le support hérité est activé après la connexion dans l'authentification au démarrage SafeGuard. 0 = Support hérité activé 1 = Support hérité non activé (standard)
ALTERNATE	Définit si les périphériques USB sont pris en charge par l'authentification au démarrage SafeGuard. 0 = prise en charge USB activée (standard) 1 = aucune prise en charge USB
NOATA	Définit si un pilote de périphérique int13 est utilisé.0 = pilote de périphérique ATA standard (par défaut)1 = pilote de périphérique int13
ACPIAPIC	Définit si la prise en charge ACPI/APIC est utilisée. 0 = aucune prise en charge ACPI/APIC (par défaut)1 = prise en charge ACPI/APIC active

13.5 Authentification au démarrage SafeGuard désactivée et Lenovo Rescue and Recovery

Si l'authentification au démarrage SafeGuard est désactivée sur l'ordinateur, l'authentification Rescue and Recovery doit être activée pour la protection contre l'accès aux fichiers chiffrés à partir de l'environnement Rescue and Recovery.

Retrouvez plus d'informations sur l'activation de l'authentification Rescue and Recovery dans la documentation Lenovo Rescue and Recovery.

14 Accès administratif aux ordinateurs d'extrémité Windows

Remarque : les descriptions suivantes se rapportent aux ordinateurs d'extrémité Windows protégés par SafeGuard Enterprise à l'aide de l'authentification au démarrage SafeGuard.

SafeGuard Enterprise utilise deux types de comptes pour permettre aux utilisateurs de se connecter aux ordinateurs d'extrémité et d'exécuter des tâches administratives après l'installation de SafeGuard Enterprise.

- **Comptes de service pour la connexion Windows**

  Grâce aux comptes de service, les utilisateurs peuvent se connecter (connexion Windows) aux ordinateurs d'extrémité après l'installation de SafeGuard Enterprise, sans avoir à activer l'authentification au démarrage SafeGuard et sans être ajoutés en tant qu'utilisateurs sur les ordinateurs. Les listes de comptes de service sont définies dans la zone **Stratégies** du SafeGuard Management Center et attribuées aux ordinateurs d'extrémité via des stratégies. Les utilisateurs figurant sur une liste de comptes de service sont considérés comme des utilisateurs invités lorsqu'ils se connectent à l'ordinateur d'extrémité.

  Remarque : les listes de comptes de service sont attribuées aux ordinateurs d'extrémité dans les stratégies. Elles doivent être attribuées dans le premier package de configuration SafeGuard Enterprise, créé pour la configuration des ordinateurs d'extrémité.

  Retrouvez plus d'informations à la section Listes de comptes de service pour la connexion Windows à la page 99.

- **Utilisateurs de l'authentification au démarrage pour connexion à l'authentification au démarrage SafeGuard**

  Les utilisateurs de l'authentification au démarrage sont des comptes locaux prédéfinis qui permettent aux utilisateurs de se connecter (connexion à l'authentification au démarrage SafeGuard) aux ordinateurs d'extrémité, une fois l'authentification au démarrage SafeGuard activée, pour effectuer des tâches administratives. Les comptes sont définis dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center (identifiant utilisateur et mot de passe) et attribués aux ordinateurs d'extrémité au moyen de groupes d'authentification au démarrage inclus dans les packages de configuration.

  Retrouvez plus d'informations à la section Utilisateurs de l'authentification au démarrage pour connexion à l'authentification au démarrage SafeGuard à la page 104.

15 Listes de comptes de service pour la connexion Windows

Remarque : les comptes de service sont uniquement pris en charge sur les ordinateurs d'extrémité Windows protégés par SafeGuard Enterprise avec l'authentification au démarrage SafeGuard.

Exemple de scénario type pour la plupart des mises en œuvre : une équipe de déploiement installe de nouveaux ordinateurs dans un environnement sur lequel SafeGuard Enterprise est installé. Pour des raisons d'installation ou de vérification, les opérateurs en charge du déploiement peuvent se connecter à leur ordinateur respectif avant que l'utilisateur final ne reçoive sa nouvelle machine et n'active l'authentification au démarrage SafeGuard.

Le scénario peut ainsi être le suivant :

1. SafeGuard Enterprise est installé sur un ordinateur d'extrémité.
2. Après le redémarrage de l'ordinateur d'extrémité, l'opérateur en charge du déploiement se connecte.
3. L'opérateur en charge du déploiement est ajouté à l'authentification au démarrage SafeGuard qui s'active. L'opérateur en charge du déploiement devient le propriétaire de l'ordinateur d'extrémité.

À la réception de son ordinateur, l'utilisateur final ne pourra pas se connecter à l'authentification au démarrage SafeGuard. L'utilisateur doit exécuter une procédure Challenge/Réponse.

Pour éviter que les opérations d'administration sur un ordinateur protégé par SafeGuard Enterprise n'activent l'authentification au démarrage SafeGuard et n'entraînent l'ajout d'opérateurs en charge du déploiement comme autant d'utilisateurs et de propriétaires de la machine, SafeGuard Enterprise vous permet de créer des listes de comptes de service pour les ordinateurs protégés par SafeGuard Enterprise. Les utilisateurs inclus dans ces listes sont traités comme des utilisateurs invités SafeGuard Enterprise.

Avec les comptes de service, le scénario est le suivant :

1. SafeGuard Enterprise est installé sur un ordinateur d'extrémité.
2. Après le redémarrage de l'ordinateur, un opérateur en charge du déploiement et figurant sur une liste de comptes de service se connecte (connexion Windows).
3. D'après la liste de comptes de service appliquée à l'ordinateur, l'utilisateur est identifié comme un compte de service et traité comme utilisateur invité.

L'opérateur en charge du déploiement n'est pas ajouté à l'authentification au démarrage SafeGuard et l'authentification au démarrage n'est pas activée. L'opérateur en charge du déploiement ne devient pas le propriétaire de l'ordinateur d'extrémité. L'utilisateur final peut se connecter et activer l'authentification au démarrage SafeGuard.

Remarque : les listes de comptes de service sont attribuées aux ordinateurs d'extrémité dans les stratégies. Elles doivent être attribuées dans le premier package de configuration SafeGuard Enterprise, créé pour la configuration des ordinateurs d'extrémité.

15.1 Création de listes de comptes de service et ajout d'utilisateurs

1. Dans la zone de navigation, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation de la stratégie, sélectionnez **Listes de comptes de service**.
3. Dans le menu contextuel de l'option **Listes de comptes de service**, cliquez sur **Nouveau** > **Liste de comptes de service**.
4. Entrez un nom pour la liste de comptes de service, puis cliquez sur **OK**.
5. Sélectionnez la nouvelle liste sous **Listes de comptes de service** dans la fenêtre de navigation de la stratégie.
6. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel de la liste de comptes de service. Dans le menu contextuel, sélectionnez **Ajouter**.

   Une nouvelle ligne utilisateur est ajoutée.

7. Entrez le **Nom d'utilisateur** et le **Nom du domaine** dans les colonnes correspondantes, puis appuyez sur **Entrée**. Répétez cette étape pour ajouter d'autres utilisateurs.
8. Enregistrez vos modifications en cliquant sur l'icône **Enregistrer** de la barre d'outils.

La liste de comptes de service est à présent enregistrée et peut être sélectionnée dès lors que vous créez une stratégie.

15.2 Informations supplémentaires pour la saisie de noms d'utilisateur et de domaine

Il existe plusieurs méthodes servant à spécifier des utilisateurs dans les listes de comptes de service. Deux champs sont alors utilisés : **Nom d'utilisateur** et **Nom du domaine**. Les restrictions s'appliquent aussi pour les entrées valides dans ces champs.

Présentation des différentes combinaisons de connexion

Les deux champs distincts **Nom d'utilisateur** et **Nom du domaine** par entrée de liste vous permettent de couvrir toutes les combinaisons disponibles de connexion, par exemple "utilisateur@domaine" ou "domaine\utilisateur".

Pour gérer plusieurs combinaisons nom d'utilisateur/nom de domaine, vous pouvez utiliser des astérisques (*) comme caractères génériques. Une astérisque peut remplacer le premier signe, le dernier signe ou être le seul signe autorisé.

Par exemple :

- **Nom d'utilisateur :** Administrateur
- **Nom du domaine :** *

Cette combinaison indique tous les utilisateurs ayant pour nom d'utilisateur Administrateur et se connectant à un poste en local ou en réseau quel qu'il soit.

Le nom du domaine prédéfini [LOCALHOST] disponible dans la liste déroulante du champ **Nom du domaine** indique une connexion à n'importe quel ordinateur en local.

Par exemple :

- **Nom d'utilisateur** : "*admin"
- **Nom du domaine** : [LOCALHOST]

Cette combinaison indique tous les utilisateurs dont le nom d'utilisateur se termine par "admin" et se connectant à un poste en local quel qu'il soit.

Les utilisateurs peuvent se connecter de différentes manières.

Par exemple :

- utilisateur : test, domaine : monentreprise ou
- utilisateur : test, domaine : monentreprise.com.

Étant donné que les spécifications de domaine dans les listes de comptes de service ne sont pas automatiquement résolues, trois méthodes possibles servant à indiquer correctement le domaine sont disponibles :

- Vous savez exactement comment l'utilisateur va se connecter et saisir le domaine en conséquence.
- Vous créez plusieurs entrées de liste de comptes de service.
- Vous utilisez les caractères génériques pour couvrir l'ensemble des cas (utilisateur : test, domaine : monentreprise*).

Remarque : afin d'éviter les problèmes liés au fait que Windows peut utiliser des noms tronqués et non la même séquence de caractères, nous vous recommandons de saisir le NomComplet et le nom NetBIOS, voire d'utiliser des caractères génériques.

Restrictions

Un astérisque ne peut remplacer que le premier signe, le dernier signe ou être le seul signe autorisé. Voici quelques exemples de chaînes valides et non valides concernant l'utilisation des astérisques :

- Exemples de chaînes valides : admin*, *, *strateur, *minis*.
- Exemple de chaînes non valides : **, Admin*trateur, Ad*minst*.

En outre, les restrictions suivantes s'appliquent :

- Le caractère ? n'est pas autorisé dans les noms de connexion utilisateur.
- Les caractères / \ [ ] : ; | = , + * ? < > " ne sont pas autorisés dans les noms de domaine.

15.3 Modification et suppression des listes de comptes de service

En tant que responsable de la sécurité possédant le droit **Modifier les listes de comptes de service**, vous pouvez modifier ou supprimer les listes de comptes de service à tout moment :

- Pour modifier une liste de comptes de service, cliquez dessus dans la fenêtre de navigation de la stratégie. La liste de comptes de service s'ouvre dans la zone d'action et vous pouvez alors ajouter, supprimer ou modifier les noms d'utilisateur dans la liste.
- Pour supprimer une liste de comptes de service, sélectionnez-la dans la fenêtre de navigation de stratégie, ouvrez le menu contextuel, puis sélectionnez **Supprimer**.

15.4 Attribution d'une liste de comptes de service dans une stratégie

1. Créez une nouvelle stratégie du type **Authentification** ou sélectionnez-en une existante.
2. Sous **Options de connexion**, sélectionnez la liste de comptes de service requise dans la liste déroulante **Liste de comptes de service**.

   Remarque : Le paramètre par défaut est [**Aucune liste**], c'est-à-dire qu'aucune liste de comptes de service ne s'applique. Les opérateurs en charge du déploiement se connectant à l'ordinateur après l'installation de SafeGuard Enterprise ne sont pas traités comme des utilisateurs invités. Ils peuvent activer l'authentification au démarrage SafeGuard et être ajoutés à l'ordinateur d'extrémité. Pour annuler l'attribution d'une liste de comptes de service, sélectionnez l'option [**Aucune liste**].
3. Enregistrez vos modifications en cliquant sur l'icône **Enregistrer** de la barre d'outils.

Vous pouvez à présent transférer la stratégie sur les ordinateurs d'extrémité concernés et y mettre à disposition les comptes de service disponibles.

Remarque : si vous sélectionnez des listes de comptes de service différentes dans des stratégies qui le sont tout autant et qui correspondent toutes au RSOP (Resulting Set of Policies, paramètre valide pour un ordinateur/groupe spécifique), la liste de comptes de service affectée à la dernière stratégie appliquée prend le dessus sur toutes les listes de comptes de service précédemment attribuées. Les listes de comptes de service ne sont pas fusionnées. Pour voir la RSOP dans **Utilisateurs et ordinateurs**, vous avez besoin au moins des droits d'accès en **Lecture seule** pour les objets concernés.

15.5 Transfert de la stratégie à l'ordinateur d'extrémité

La fonctionnalité de liste de comptes de service se révèle tout particulièrement utile et importante durant l'installation initiale, au cours de la phase de déploiement d'une mise en œuvre. C'est pourquoi nous conseillons le transfert des paramètres de liste de comptes de service sur l'ordinateur d'extrémité, sitôt l'installation effectuée. Pour rendre disponible la liste des comptes de service sur l'ordinateur d'extrémité à ce moment précis, ajoutez une stratégie de type **Authentification** lors de la création du package de configuration initiale pour pouvoir configurer l'ordinateur d'extrémité après l'installation.

Vous pouvez à tout moment changer les paramètres de la liste des comptes de service, créer une nouvelle stratégie et la transférer sur les ordinateurs d'extrémité.

15.6 Connexion à un ordinateur d'extrémité à l'aide d'un compte de service

Lors de la première connexion à Windows après le redémarrage de l'ordinateur, un utilisateur figurant sur une liste de comptes de service se connecte à l'ordinateur en tant qu'utilisateur invité SafeGuard Enterprise. Cette première connexion Windows à l'ordinateur d'extrémité ne déclenche pas de procédure d'authentification au démarrage SafeGuard, de même qu'elle n'ajoute pas l'utilisateur à l'ordinateur. L'infobulle de l'icône de la barre d'état système SafeGuard Enterprise "Synchronisation utilisateur initiale terminée" n'apparaît pas.

Affichage de l'état du compte de service sur l'ordinateur d'extrémité

L'état de connexion de l'utilisateur invité est également disponible via l'icône de la barre d'état système. Retrouvez plus d'informations dans le *Manuel d'utilisation de SafeGuard Enterprise* au chapitre *Icône de la barre d'état système et infobulle* (description du champ sur l'**État de l'utilisateur SGN**).

15.7 Journalisation des événements

Les actions accomplies concernant les listes de comptes de service sont signalées par les événements du journal suivants :

SafeGuard Management Center

- Liste de comptes de service <nom> créée
- Liste de comptes de service <nom> modifiée
- Liste de comptes de service <nom> supprimée

Ordinateurs d'extrémité protégés par SafeGuard Enterprise

- Utilisateur Windows <nom domaine/utilisateur> connecté à <horodatage> sur le poste <nom domaine/poste de travail> avec un compte de service SGN.
- Nouvelle liste de comptes de service <nom> importée.
- Liste de comptes de service <nom> supprimée.

16 Utilisateurs de l'authentification au démarrage pour connexion à l'authentification au démarrage SafeGuard

Remarque : les utilisateurs de l'authentification au démarrage sont uniquement pris en charge sur les ordinateurs d'extrémité Windows protégés par SafeGuard Enterprise avec l'authentification au démarrage SafeGuard.

Une fois SafeGuard Enterprise installé et l'authentification au démarrage SafeGuard activée, vous devez pouvoir accéder aux ordinateurs d'extrémité pour exécuter des tâches administratives. Grâce aux utilisateurs de l'authentification au démarrage, les utilisateurs (notamment des membres de l'équipe informatique) peuvent se connecter aux ordinateurs d'extrémité à l'authentification au démarrage SafeGuard, pour exécuter des tâches administratives, sans avoir à lancer de procédure Challenge/Réponse. Il n'y a pas de connexion automatique à Windows. Les utilisateurs se connectant avec leurs comptes utilisateur d'authentification au démarrage doivent se connecter à Windows avec leurs comptes Windows existants.

Vous pouvez créer des utilisateurs de l'authentification au démarrage, les regrouper dans des groupes de l'authentification au démarrage et attribuer ces groupes à des ordinateurs d'extrémité. Les utilisateurs inclus dans le groupe de l'authentification au démarrage, sont ajoutés à l'authentification au démarrage SafeGuard et peuvent se connecter à l'aide de leur nom d'utilisateur et de leur mot de passe prédéfinis.

Remarque : pour gérer les utilisateurs et les groupes de l'authentification au démarrage, vous avez besoin des droits d'**Accès complet** pour le nœud **POA** sous **Utilisateurs et ordinateurs**.

16.1 Création d'utilisateurs POA

Pour créer des utilisateurs POA, vous avez besoin des droits d'**Accès complet** pour le nœud **POA** sous **Utilisateurs et ordinateurs**.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, sous **POA**, sélectionnez **Utilisateurs POA**.
3. Dans le menu contextuel des **Utilisateurs POA**, cliquez sur **Nouveau** > **Créer un utilisateur**.

   La boîte de dialogue **Créer un utilisateur** s'affiche.

4. Dans le champ **Nom complet**, saisissez un nom, par exemple le nom de connexion du nouvel utilisateur de l'authentification au démarrage.
5. Vous pouvez également saisir une description pour le nouvel utilisateur de l'authentification au démarrage.

6. Saisissez un mot de passe pour le nouvel utilisateur de l'authentification au démarrage et confirmez-le.

   Remarque : pour renforcer la sécurité, le mot de passe doit respecter des exigences de complexité minimales, à savoir une longueur minimale de 8 caractères, un mélange de caractères numériques et alphanumériques, etc. Si le mot de passe que vous avez entré est trop court, un message d'avertissement s'affiche.

7. Cliquez sur **OK**.

Le nouvel utilisateur POA est créé et apparaît sous **Utilisateurs POA** dans la zone de navigation **Utilisateurs et ordinateurs**.

16.2 Modification du mot de passe d'un utilisateur de l'authentification au démarrage

Pour modifier les utilisateurs de l'authentification au démarrage, vous avez besoin des droits d'**Accès complet** pour le nœud **POA** sous **Utilisateurs et ordinateurs**.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, sous **POA**, **Utilisateurs POA**, sélectionnez l'utilisateur de l'authentification au démarrage approprié.
3. Dans le menu contextuel de cet utilisateur de l'authentification au démarrage, sélectionnez **Propriétés**.

   La boîte de dialogue Propriétés de l'utilisateur de l'authentification au démarrage s'affiche.

4. Dans l'onglet **Général**, sous **Mot de passe utilisateur**, saisissez le nouveau mot de passe et confirmez-le.
5. Cliquez sur **OK**.

Le nouveau mot de passe est appliqué à l'utilisateur de l'authentification au démarrage correspondant.

16.3 Suppression des utilisateurs de l'authentification au démarrage

Pour supprimer les utilisateurs de l'a, vous avez besoin des droits d'**Accès complet** pour le nœud **POA** sous **Utilisateurs et ordinateurs.**

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, sous **POA**, **Utilisateurs POA**, sélectionnez l'utilisateur de l'authentification au démarrage approprié.
3. Cliquez avec le bouton droit de la souris sur l'utilisateur de l'authentification au démarrage et sélectionnez **Supprimer** dans le menu contextuel.

L'utilisateur de l'authentification au démarrage est supprimé. Il n'apparaît plus dans la fenêtre de navigation **Utilisateurs et ordinateurs**.

Remarque : si l'utilisateur appartient à un ou plusieurs groupes d'authentification au démarrage, l'utilisateur de l'authentification au démarrage est également supprimé de tous les groupes. L'utilisateur de l'authentification au démarrage reste cependant disponible sur l'ordinateur d'extrémité jusqu'à ce que le groupe d'authentification au démarrage ait été attribué.

16.4 Création de groupes POA

Pour créer des groupes POA, vous avez besoin des droits d'**Accès complet** pour le noeud **POA** sous **Utilisateurs et ordinateurs**.

Pour attribuer des utilisateurs de l'authentification au démarrage aux ordinateurs d'extrémité, les comptes doivent être réorganisés en groupes.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation **Utilisateurs et ordinateurs**, sous **POA**, sélectionnez **Groupes POA**.
3. Dans le menu contextuel des **Groupes POA**, cliquez sur **Nouveau** > **Créer un groupe**.

   La boîte de dialogue **Créer un groupe** s'affiche.
4. Dans le champ **Nom complet**, saisissez le nom du nouveau groupe POA.
5. Ajoutez éventuellement une description.
6. Cliquez sur **OK**.

Le nouveau groupe POA est créé. Il apparaît sous **Groupes POA** dans la zone de navigation **Utilisateurs et ordinateurs**. Vous pouvez maintenant ajouter des utilisateurs POA au groupe POA.

16.5 Ajout d'utilisateurs dans les groupes POA

Pour modifier les groupes POA, vous avez besoin des droits d'**Accès complet** pour le noeud **POA** sous **Utilisateurs et ordinateurs**.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, sous **POA**, **Groupes POA**, sélectionnez le groupe POA approprié.

   Dans la zone d'action du SafeGuard Management Center, sur la droite, l'onglet **Membres** s'affiche.
3. Dans la barre d'outils du SafeGuard Management Center, cliquez sur l'icône **Ajouter** (signe + vert).

   La boîte de dialogue **Sélectionner un objet membre** s'affiche.
4. Sélectionnez l'utilisateur que vous souhaitez ajouter au groupe.
5. Cliquez sur **OK**.

L'utilisateur POA est ajouté au groupe, puis affiché dans l'onglet **Membres**.

16.6 Suppression d'utilisateurs de groupes POA

Pour modifier les groupes POA, vous avez besoin des droits d'**Accès complet** pour le noeud **POA** sous **Utilisateurs et ordinateurs**.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, sous **POA**, **Groupe POA**, sélectionnez le groupe d'authentification au démarrage approprié.

   Dans la zone d'action du SafeGuard Management Center, sur la droite, l'onglet **Membres** s'affiche.
3. Sélectionnez l'utilisateur que vous souhaitez supprimer du groupe.
4. Dans la barre d'outils du SafeGuard Management Center, cliquez sur l'icône **Supprimer** (croix rouge).

L'utilisateur est supprimé du groupe.

16.7 Attribution d'utilisateurs de l'authentification au démarrage aux ordinateurs d'extrémité

Remarque : pour attribuer des utilisateurs de l'authentification au démarrage aux ordinateurs d'extrémité, les comptes doivent être réorganisés en groupes.

La façon dont vous attribuez et annulez l'attribution des utilisateurs de l'authentification au démarrage aux ordinateurs d'extrémité dépend du type d'ordinateur :

- Pour les **ordinateurs d'extrémité administrés**, les groupes d'authentification au démarrage peuvent être attribués dans l'onglet **Attribution de groupe d'authentification au démarrage** dans **Utilisateurs et ordinateurs**.
- Pour les **ordinateurs d'extrémité non administrés** qui fonctionnent en mode autonome et ne sont pas connectés au serveur SafeGuard Enterprise, un package de configuration avec un groupe d'authentification au démarrage doit être créé et déployé.

16.7.1 Attribution d'utilisateurs de l'authentification au démarrage aux ordinateurs d'extrémité administrés

Pour attribuer des utilisateurs de l'authentification au démarrage aux ordinateurs administrés, vous avez besoin des droits d'**Accès complet** ou en **Lecture seule** pour le groupe d'authentification au démarrage concerné et des droits d'**Accès complet** pour les conteneurs correspondants.

Remarque : l'attribution d'utilisateurs de l'authentification au démarrage est seulement valide pour les ordinateurs d'extrémité SafeGuard Enterprise administrés à partir de la version 5.60.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, sélectionnez le conteneur requis.
3. Dans la zone d'action du SafeGuard Management Center, sélectionnez l'onglet **Attribution de groupe d'authentification au démarrage**.

   Sous **Groupes POA** à droite, tous les groupes d'authentification au démarrage disponibles apparaissent.

4. Faites glisser le groupe d'authentification au démarrage requis des **Groupes POA** dans la zone d'action **Attribution de groupe d'authentification au démarrage**.

   Le **Nom du groupe** et le **Groupe DSN** du groupe d'authentification au démarrage apparaissent dans la zone de travail.

5. Enregistrez vos changements dans la base de données.

Tous les membres du groupe d'authentification au démarrage attribué sont déployés sur tous les ordinateurs d'extrémité dans le conteneur sélectionné.

Vous pouvez annuler l'attribution d'un groupe d'authentification au démarrage ou changer le groupe d'authentification au démarrage attribué en continuant comme indiqué et en déplaçant les groupes de l'onglet **Attribution de groupe d'authentification au démarrage** et de la zone **Groupes POA** depuis la zone d'action et vers celle-ci.

Après avoir enregistré vos changements dans la base de données, la nouvelle attribution s'applique.

16.7.2 Attribution d'utilisateurs de l'authentification au démarrage aux ordinateurs d'extrémité non administrés

Pour attribuer les utilisateurs de l'authentification au démarrage aux ordinateurs d'extrémité non administrés, vous avez besoin des droits en **Lecture seule** ou d'**Accès complet** pour le groupe d'authentification au démarrage concerné.

Les utilisateurs de l'authentification au démarrage sont attribués aux ordinateurs d'extrémité non administrés (ordinateurs fonctionnant en mode autonome) dans les packages de configuration.

1. Dans SafeGuard Management Center, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Sélectionnez un package de configuration existant ou créez-en un nouveau.
3. Indiquez un **Groupe d'authentification au démarrage** créé auparavant dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center qui sera appliqué aux ordinateurs d'extrémité.

   Un groupe **aucune liste** est disponible pour la sélection par défaut. Ce groupe peut être utilisé pour supprimer une attribution de groupe d'authentification au démarrage sur les ordinateurs d'extrémité.

4. Indiquez un chemin de sortie pour le package de configuration.
5. Cliquez sur **Créer un package de configuration**.
6. Déployez le package de configuration sur les ordinateurs d'extrémité.

L'installation du package de configuration entraîne l'ajout des utilisateurs inclus dans le groupe à l'authentification au démarrage SafeGuard sur les ordinateurs d'extrémité. Les utilisateurs de l'authentification au démarrage sont disponibles pour la connexion à l'authentification au démarrage.

Remarque : lorsque vous mettez à niveau des ordinateurs d'extrémité non administrés pour qu'ils soient administrés, les utilisateurs de l'authentification au démarrage restent actifs, s'ils ont aussi été attribués dans SafeGuard Management Center. Les mots de passe définis dans les groupes d'authentification au démarrage déployés dans les packages de configuration sont définis sur ceux spécifiés dans SafeGuard Management Center. Les mots de passe changés avec **F8** sont remplacés. Retrouvez plus d'informations sur la mise à niveau des ordinateurs d'extrémité non administrés dans le *Guide de mise à niveau de SafeGuard Enterprise*.

16.7.3 Annulation de l'attribution d'utilisateurs de l'authentification au démarrage des ordinateurs d'extrémité non administrés

Les utilisateurs de l'authentification au démarrage peuvent être supprimés des ordinateurs d'extrémité en attribuant un groupe d'authentification au démarrage vide :

1. Dans SafeGuard Management Center, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Sélectionnez un package de configuration existant ou créez-en un nouveau.
3. Spécifiez un **Groupe POA** vide créé préalablement dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center, ou sélectionnez le groupe d'authentification au démarrage **aucune liste**disponible par défaut dans l'**Outil de package de configuration**.
4. Indiquez un chemin de sortie pour le package de configuration.
5. Cliquez sur **Créer un package de configuration**.
6. Déployez le package de configuration sur les ordinateurs d'extrémité.

L'installation du package de configuration entraîne la suppression de tous les utilisateurs de l'authentification au démarrage des ordinateurs d'extrémité. Tous les utilisateurs concernés sont donc supprimés de l'authentification au démarrage.

16.7.4 Modification des attributions d'utilisateurs de l'authentification au démarrage sur les ordinateurs d'extrémité non administrés

1. Créez un nouveau groupe POA ou modifiez-en un existant.
2. Créez un nouveau package de configuration et sélectionnez le nouveau groupe d'authentification au démarrage ou celui qui a été modifié.
3. Déployez le nouveau package de configuration sur l'ordinateur d'extrémité.

Le nouveau groupe d'authentification au démarrage est disponible sur l'ordinateur d'extrémité. Tous les utilisateurs inclus sont ajoutés à l'authentification au démarrage. Le nouveau groupe remplace le précédent. Les groupes POA ne sont pas fusionnés.

16.8 Connexion à un ordinateur d'extrémité à l'aide d'un utilisateur de l'authentification au démarrage

1. Mettez l'ordinateur sous tension.

   La boîte de dialogue de connexion de l'authentification au démarrage SafeGuard s'affiche.

2. Saisissez le **Nom d'utilisateur** et le **Mot de passe** de l'utilisateur POA prédéfini.

   Vous n'êtes pas connecté à Windows automatiquement. La boîte de dialogue de connexion de Windows s'affiche.

3. Dans le champ **Domaine**, sélectionnez le domaine <**Authentification au démarrage**>.
4. Connectez-vous à Windows à l'aide de votre compte utilisateur Windows existant.

16.8.1 Changement du mot de passe local

Si le mot de passe d'un utilisateur de l'authentification au démarrage a été changé avec **F8**, le changement n'est pas synchronisé avec d'autres ordinateurs d'extrémité. L'administrateur doit changer de manière centralisée le mot de passe pour cet utilisateur.

17 Paramètres de stratégie

Les stratégies SafeGuard Enterprise comportent tous les paramètres nécessaires pour mettre en œuvre une stratégie de sécurité à l'échelle de l'entreprise sur les ordinateurs d'extrémité.

Les stratégies de SafeGuard Enterprise peuvent comporter des paramètres pour les domaines suivants (types de stratégies) :

- **Paramètres généraux**

  Paramètres pour le taux de transfert, la personnalisation, la récupération de connexion, les images d'arrière-plan, etc.

- **Authentification**

  Paramètres de mode de connexion, verrouillage de périphérique, etc.

- **PIN**

  Définit la configuration minimale des codes PIN utilisés.

- **Mots de passe**

  Définit la configuration minimale des mots de passe utilisés.

- **Phrase secrète**

  Définit la configuration minimale pour les phrases secrètes utilisées pour SafeGuard Data Exchange.

- **Protection des périphériques**

  Paramètres de chiffrement basé sur volume ou sur fichier (y compris des paramètres pour SafeGuard Data Exchange, SafeGuard Cloud Storage et SafeGuard Portable) : algorithmes, clés, les lecteurs sur lesquels les données doivent être chiffrées, etc.

- **Paramètres de machine spécifiques**

  Paramètres d'authentification au démarrage SafeGuard (activer/désactiver), d'éveil par appel réseau sécurisé, d'options d'affichage, etc.

- **Journalisation**

  Définit les événements à consigner dans le journal et leurs destinations de sortie.

- **Protection de la configuration**

  Remarque : le paramètre Protection de la configuration n'est disponible que pour les clients SafeGuard Enterprise jusqu'à la version 6.0. La stratégie est disponible dans la version 6.1 de SafeGuard Management Center afin de prendre en charge les clients de la version 6.0 de SafeGuard Enterprise qui ont installé la Protection de la configuration et qui veulent l'administrer avec la version 6.1 du Management Center. La Protection de la configuration n'est pas prise en charge pour les ordinateurs d'extrémité sur lesquels SafeGuard Enterprise 6.1 est installé.

Paramètres (autoriser/bloquer) pour l'utilisation des ports et des périphériques (lecteurs multimédias amovibles, imprimantes, etc.).

- **Chiffrement de fichier**

  Paramètres pour un chiffrement basé sur fichier sur les lecteurs locaux et les emplacements réseau, surtout pour les groupes de travail et les partages réseau.

Dans SafeGuard Management Center, les stratégies par défaut sont disponibles pour tous les types de stratégie. Dans les stratégies **Protection des périphériques**, les stratégies de chiffrement intégral du disque (cible : périphériques de stockage de masse), Cloud Storage (cible : DropBox) et Data Exchange (cible : périphériques de stockage de masse) sont disponibles. Les options dans ces stratégies par défaut sont définies sur les valeurs adéquates. Vous pouvez modifier les paramètres par défaut en fonction de vos exigences particulières. Les stratégies par défaut sont nommées <type de stratégie> (Par défaut).

Remarque : les noms de ces stratégies par défaut dépendent du paramètre de langue définit au cours de l'installation. Si vous modifiez la langue du SafeGuard Management Center par la suite, les noms de la stratégie par défaut demeurent dans le paramètre de langue au cours de l'installation.

17.1 Paramètres généraux

Paramètre de stratégie	Explication
CHARGEMENT DE PARAMÈTRES	
Mode de récursivité des stratégies	**Paramètres de relecture de la machine** Si **Paramètres de relecture de la machine** est sélectionné pour une stratégie dans le champ **Mode de récursivité des stratégies** et si la stratégie provient d'une machine (le paramètre **Paramètres de relecture de la machine** d'une stratégie utilisateur n'entraîne aucun effet), cette stratégie est mise en œuvre une nouvelle fois à la fin. Ceci remplace ensuite les paramètres de l'utilisateur et les paramètres de la machine s'appliquent. **Ignorer l'utilisateur** Si vous sélectionnez **Ignorer l'utilisateur** pour une stratégie (stratégie de machine) dans le champ **Mode de récursivité des stratégies**, et si la stratégie provient d'une machine, seuls les paramètres de la machine sont analysés. Les paramètres de l'utilisateur ne sont pas analysés. **Aucun bouclage** **Aucun blocage** est le comportement standard : Les stratégies de l'utilisateur sont prioritaires sur celles de la machine. **Comment les paramètres "Ignorer l'utilisateur" et "Paramètres de relecture de la machine" sont-ils analysés?** S'il existe des attributions de stratégies actives, les stratégies de la machine sont analysées et regroupées d'abord. Si le regroupement

Paramètre de stratégie	Explication
	des différentes stratégies se traduit par l'attribut **Ignorer l'utilisateur** dans le mode de récursivité des stratégies, les stratégies qui auraient été appliquées pour l'utilisateur ne sont plus analysées. Cela signifie que les mêmes stratégies s'appliquent à l'utilisateur et à la machine. Si la valeur **Paramètres de relecture de la machine** est appliquée dans le cas du mode de récursivité des stratégies, lorsque les stratégies individuelles de la machine ont été regroupées, les stratégies de l'utilisateur sont ensuite combinées à celles de la machine. Après le regroupement, les stratégies de la machine sont réécrites et remplacent les paramètres de stratégie de l'utilisateur. Cela signifie que, si un paramètre est présent dans les deux stratégies, la valeur de la stratégie de la machine remplace celle de la stratégie de l'utilisateur. Si le regroupement des stratégies individuelles de la machine produit la valeur standard, par défaut, les conditions suivantes s'appliquent : Les paramètres de l'utilisateur deviennent prioritaires sur ceux de la machine.
TAUX DE TRANSFERT	
Intervalle de connexion au serveur (min)	Détermine la période, en minutes, après laquelle un client SafeGuard Enterprise envoie une demande de stratégie (modifications) au serveur SafeGuard Enterprise. **Remarque :** pour éviter qu'un grand nombre de clients ne contactent le serveur simultanément, la communication s'effectue toujours dans une période de +/- 50% de l'intervalle de connexion défini. Exemple : le paramètre “90 minutes” se traduit par une période de communication entre le client et le serveur de 45 à 135 minutes.
JOURNALISATION	
Commentaires après plusieurs événements	Le système de journalisation, introduit sous le nom de Win32 Service “SGM LogPlayer”, recueille les entrées du journal générées par SafeGuard Enterprise pour la base de données centrale et les stocke dans des fichiers journaux locaux. Elles sont stockées dans le cache local dans le répertoire “Auditing\SGMTransLog”. Ces fichiers sont transférés au mécanisme de transport qui les envoie ensuite à la base de données via le serveur SGN. Le transfert s'effectue dès que le mécanisme de transport a réussi à créer une connexion au serveur. La taille du fichier journal a donc tendance à augmenter jusqu'à ce qu'une connexion ait été établie. Pour limiter la taille de chaque fichier journal, il est possible de spécifier un nombre maximal d'entrées du journal dans la stratégie. Lorsque le nombre d'entrées prédéfini a été atteint, le système de journalisation place le fichier journal dans la file d'attente de transport du serveur SGN et démarre un nouveau fichier journal.

Paramètre de stratégie	Explication
PERSONNALISATION	
Langue utilisée sur le client	Langue dans laquelle les paramètres de SafeGuard Enterprise sont affichés sur l'ordinateur d'extrémité : Vous pouvez sélectionner une langue prise en charge ou le paramètre de langue du système d'exploitation de l'ordinateur d'extrémité.
RÉCUPÉRATION DE LA CONNEXION	
Activer la récupération de connexion après la corruption du cache local Windows	Le cache local Windows représente le point de départ et de fin de l'échange de données entre l'ordinateur d'extrémité et le serveur. Il stocke la totalité des clés, stratégies, certificats utilisateur et fichiers d'audit. Les données stockées dans le cache local sont signées et ne peuvent pas être modifiées manuellement. La récupération de connexion après corruption du cache local est désactivée par défaut. En d'autres termes, le cache local Windows sera restauré automatiquement à partir de sa sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local Windows. Si le cache local Windows doit être réparé explicitement via une procédure Challenge/Réponse, définissez ce champ sur **Oui**.
Local Self Help	
Activer Local Self Help	Détermine si les utilisateurs sont autorisés à se connecter à leurs ordinateurs avec Local Self Help en cas d'oubli de leur mot de passe. Avec Local Self Help, l'utilisateur peut se connecter en répondant à un nombre spécifique de questions prédéfinies dans l'authentification au démarrage SafeGuard. Il peut de nouveau accéder à son ordinateur même si aucune connexion téléphonique ou Internet n'est disponible. **Remarque :** la connexion automatique à Windows doit être activée pour que l'utilisateur puisse utiliser Local Self Help. Dans le cas contraire, Local Self Help ne fonctionne pas.
Longueur minimum des réponses	Définit la longueur minimale de caractères pour les réponses Local Self Help.
Texte de bienvenue sous Windows	Indique le texte personnalisé à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur l'ordinateur d'extrémité. Avant de pouvoir spécifier le texte ici, il doit être créé et enregistré dans la **zone de navigation des stratégies** sous **Texte d'informations**.
L'utilisateur peut définir des questions personnalisées	En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles répondre et les distribuer sur l'ordinateur d'extrémité dans la stratégie. Toutefois,

Paramètre de stratégie	Explication
	vous pouvez également accorder aux utilisateurs le droit de définir des questions personnalisées. Pour autoriser les utilisateurs à définir leurs propres questions, sélectionnez **Oui**.
Challenge / Réponse (C/R)	
Activer la récupération de la connexion (via C/R)	Détermine si un utilisateur est autorisé à générer un challenge dans l'authentification au démarrage SafeGuard afin de pouvoir accéder de nouveau à son ordinateur avec une procédure Challenge/Réponse. **Oui** : L'utilisateur est autorisé à générer un challenge. Dans ce cas, l'utilisateur peut de nouveau accéder à son ordinateur avec une procédure C/R en cas d'urgence. **Non** : L'utilisateur n'est pas autorisé à générer un challenge. Dans ce cas, l'utilisateur ne peut pas exécuter une procédure C/R pour accéder de nouveau à son ordinateur en cas d'urgence.
Autoriser la connexion Windows automatique	Permet à l'utilisateur de se connecter automatiquement à Windows après s'être authentifié avec la procédure Challenge/Réponse. **Oui** : l'utilisateur est automatiquement connecté à Windows. **Non** : l'écran de connexion Windows apparaît. **Exemple** : un utilisateur a oublié son mot de passe. Après la procédure Challenge/Réponse, SafeGuard Enterprise connecte l'utilisateur à l'ordinateur sans mot de passe SafeGuard Enterprise. Dans ce cas, la connexion automatique à Windows est désactivée et l'écran de connexion Windows s'affiche. L'utilisateur ne peut pas se connecter car il ne connaît pas le mot de passe SafeGuard Enterprise (=mot de passe Windows). Le paramètre **Oui** autorise la connexion automatique ; l'utilisateur n'est pas bloqué au niveau de l'écran de connexion Windows.
Texte d'informations	Affiche un texte d'informations lorsqu'une procédure Challenge/Réponse est lancée dans l'authentification au démarrage SafeGuard. Par exemple : "Veuillez contacter le bureau de support en appelant le 03 20 90 27 29." Avant d'insérer un texte ici, vous devez le créer sous forme de fichier texte dans la **zone de navigation de stratégie** sous **Texte d'informations**.
IMAGES	
	Condition préalable : Les nouvelles images doivent être enregistrées dans la **zone de navigation des stratégies** du SafeGuard Management Center sous **Images**. Les images ne sont disponibles qu'une fois enregistrées. Formats pris en charge : .BMP, .PNG, .JPEG.

Paramètre de stratégie	Explication
Image d'arrière-plan dans l'authentification au démarrage **Image d'arrière-plan dans l'authentification au démarrage (basse résolution)**	Remplace l'arrière-plan SafeGuard Enterprise bleu par une image d'arrière-plan personnalisée. Par exemple, les clients peuvent utiliser le logo de l'entreprise dans l'authentification au démarrage SafeGuard et lors de la connexion à Windows. Taille de fichier maximale pour toutes les images bitmap d'arrière-plan : 500 Ko. Normal : ■ Résolution : 1024 x 768 (mode VESA) ■ Couleurs : illimité Basse : ■ Résolution : 640 x 480 (mode VGA) ■ Couleurs : 16 couleurs
Image de connexion dans la POA **Image de connexion dans la POA (basse résolution)**	Remplace l'image SafeGuard Enterprise affichée lors de la connexion à l'authentification au démarrage SafeGuard par une image personnalisée, par exemple le logo d'une entreprise. Normal : ■ Résolution : 413 x 140 pixels ■ Couleurs : illimité Basse : ■ Résolution : 413 x 140 pixels ■ Couleurs : 16 couleurs
Chiffrement de fichier	
Applications fiables	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez indiquer des applications comme sécurisées pour leur accorder l'accès aux fichiers chiffrés. Ceci s'avère utile, par exemple, pour activer le logiciel antivirus afin de contrôler les fichiers chiffrés. Saisissez les applications que vous voulez définir comme fiables dans la zone de liste d'édition de ce champ. Les applications doivent être saisies comme des chemins pleinement qualifiés.
Applications ignorées	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez indiquer des applications comme ignorées pour les exempter du chiffrement/déchiffrement des fichiers transparents. Par exemple, si vous définissez un programme de sauvegarde comme une application ignorée, les données chiffrées sauvegardées par le programme restent chiffrées.

Paramètre de stratégie	Explication
	Saisissez les applications que vous voulez définir comme ignorées dans la zone de liste d'édition de ce champ. Les applications doivent être saisies comme des chemins pleinement qualifiés.
Périphériques ignorés	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez exclure des périphériques entiers (par exemple, des disques) du chiffrement basé sur fichier. Dans la zone de liste d'édition, sélectionnez **Réseau** pour sélectionner un périphérique prédéfini ou saisissez les noms de périphériques requis pour exclure des périphériques données du chiffrement.
Activer le chiffrement permanent	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez configurer le chiffrement permanent. Avec le chiffrement permanent, les copies des fichiers chiffrés seront chiffrées, même lorsqu'elles sont enregistrées dans un emplacement non couvert par une règle de chiffrement. Ce paramètre de stratégie est activé par défaut.
L'utilisateur est autorisé à définir les clés par défaut	Pour le chiffrement basé sur fichier par Cloud Storage, vous pouvez décider si l'utilisateur est autorisé ou non à définir une clé par défaut pour le chiffrement. S'il est autorisé, la commande **Définir la clé par défaut** est ajoutée dans le menu contextuel Windows Explorer des dossiers de synchronisation Cloud Storage. Les utilisateurs peuvent utiliser la commande pour spécifier des clés par défaut distinctes à utiliser pour le chiffrement des différents dossiers de synchronisation.

17.2 Authentification

Paramètre de stratégie	Explication
ACCÈS	
L'utilisateur peut uniquement initialiser à partir du disque dur interne	**Remarque :** ce paramètre est uniquement pris en charge par les ordinateurs d'extrémité sur lesquels une version antérieure à la version 6.1 de SafeGuard Enterprise est installée. Il était utilisé pour permettre la récupération et autoriser l'utilisateur à démarrer l'ordinateur d'extrémité à partir d'un support externe. Ce paramètre n'est plus appliqué sur les ordinateurs d'extrémité à partir de la version 6.1. Pour le scénario de récupération concerné, vous pouvez utiliser la récupération avec des clients virtuels. Retrouvez plus d'informations à la

Paramètre de stratégie	Explication
	section Challenge/Réponse à l'aide de clients virtuels à la page 231. Détermine si les utilisateurs peuvent démarrer l'ordinateur à partir du disque dur et/ou d'un autre support. **OUI** : les utilisateurs peuvent initialiser à partir du disque dur uniquement. L'authentification au démarrage SafeGuard n'offre pas la possibilité de démarrer l'ordinateur avec une disquette ou d'autres supports externes. **NON** : les utilisateurs peuvent démarrer l'ordinateur à partir du disque dur, d'une disquette ou d'un support externe (USB, CD, etc.).
OPTIONS DE CONNEXION	
Mode de connexion	Détermine comment les utilisateurs doivent s'authentifier à l'authentification au démarrage SafeGuard. ■ **ID utilisateur/Mot de passe** les utilisateurs doivent se connecter avec leurs noms d'utilisateur et leurs mots de passe. ■ **Token** L'utilisateur peut uniquement se connecter à l'authentification au démarrage SafeGuard à l'aide d'un token ou d'une carte à puce. Ce processus offre un niveau de sécurité plus élevé. L'utilisateur doit insérer sa clé lors de la connexion. L'identité de l'utilisateur est vérifiée par la possession de la clé et la présentation du code PIN. Après la saisie d'un code PIN correct, SafeGuard Enterprise lit automatiquement les données pour la connexion de l'utilisateur. **Remarque :** lorsque ce processus de connexion a été sélectionné, les utilisateurs ne peuvent se connecter qu'en utilisant une clé préalablement générée. Vous pouvez combiner les paramètres **Identifiant utilisateur/Mot de passe** et **token.** Pour vérifier si la connexion fonctionne en utilisant un token, sélectionnez tout d'abord les deux paramètres. Dessélectionnez seulement le mode de connexion **Identifiant utilisateur/Mot de passe** si l'authentification à l'aide du token a réussi. Vous devez aussi combiner les deux paramètres, si vous voulez autoriser Local Self Help pour la connexion avec le token. ■ **Empreinte digitale** sélectionnez ce paramètre pour permettre la connexion à l'aide du lecteur d'empreintes digitales Lenovo. Les utilisateurs auxquels cette stratégie s'applique peuvent alors se connecter à l'aide d'une empreinte digitale ou d'un nom

Paramètre de stratégie	Explication
	d'utilisateur et d'un mot de passe. Cette procédure offre le niveau de sécurité maximum. Lors de la connexion, les utilisateurs font glisser leurs doigts sur le lecteur d'empreintes digitales. Lorsque l'empreinte digitale est correctement reconnue, le processus d'authentification au démarrage SafeGuard lit les codes d'accès de l'utilisateur et connecte l'utilisateur à l'authentification au démarrage. Le système transfère alors les codes d'accès vers Windows et connecte l'utilisateur à l'ordinateur. **Remarque :** après avoir sélectionné cette procédure de connexion, l'utilisateur peut se connecter uniquement à l'aide d'une empreinte digitale préenregistrée ou d'un nom d'utilisateur et d'un mot de passe. Vous ne pouvez pas utiliser conjointement les procédures de connexion par token et par empreinte digitale sur le même ordinateur.
Options de connexion à l'aide d'un token	Détermine le type de token ou de carte à puce à utiliser sur l'ordinateur d'extrémité. ■ **Non cryptographique** : Identification à l'authentification au démarrage SafeGuard et Windows basée sur les codes d'accès utilisateur. ■ **Kerberos** : Authentification basée sur les certificats à l'authentification au démarrage SafeGuard et Windows. Pour les ordinateurs d'extrémité administrés, le responsable de la sécurité émet un certificat dans une infrastructure de clé publique (PKI) et la stocke sur le token. Ce certificat est importé sous forme de certificat utilisateur dans la base de données SafeGuard Enterprise. Si un certificat généré automatiquement existe déjà dans une base de données, il est remplacé par le certificat importé. Les tokens cryptographiques ne peuvent pas être utilisés pour les ordinateurs d'extrémité non administrés. ■ **Remarque :** en cas de problèmes de connexion avec un token Kerberos, il n'est pas possible d'utiliser la procédure Challenge/Réponse ou Local Self Help pour la récupération de la connexion. Seule la procédure Challenge/Réponse utilisant les clients virtuels est prise en charge. Elle permet aux utilisateurs de récupérer l'accès aux volumes chiffrés sur leurs ordinateurs d'extrémité.
Code PIN utilisé pour la connexion automatique avec token	Indiquez un code PIN par défaut pour autoriser la connexion automatique de l'utilisateur à l'authentification au démarrage SafeGuard à l'aide d'un token ou d'une carte à puce. L'utilisateur doit insérer le token lors de la connexion et il est ensuite

Paramètre de stratégie	Explication
	connecté par le biais de l'authentification au démarrage SafeGuard. Windows démarre. Il n'est pas nécessaire de suivre les règles relatives au code PIN. **Remarque :** ■ Cette option n'est disponible que si vous sélectionnez **Token** comme **Mode de connexion**. ■ Si cette option est sélectionnée, **Connexion automatique vers Windows** doit être défini sur **Désactiver la connexion automatique vers Windows**.
Afficher les échecs de connexion pour cet utilisateur	Affiche (paramètre : **Oui**) après la connexion à l'authentification au démarrage SafeGuard et Windows, une boîte de dialogue indiquant des informations relatives au dernier échec de connexion (nom d'utilisateur/date/heure).
Afficher la dernière connexion utilisateur	Affiche (paramètre : **Oui**) après la connexion à partir de l'authentification au démarrage SafeGuard et Windows, une boîte de dialogue s'affiche contenant des informations concernant ■ la dernière connexion (nom d'utilisateur/date/heure) ; ■ les derniers codes d'accès de l'utilisateur connecté.
Désactiver la déconnexion forcée dans le verrouillage du poste de travail	**Remarque :** ce paramètre ne s'applique que sous Windows XP. Windows XP n'est plus pris en charge à partir de SafeGuard Enterprise 6.1. Ce paramètre de stratégie est toujours disponible dans SafeGuard Management Center afin de prendre en charge les clients SafeGuard Enterprise 6 administrés par la version 6.1 du Management Center. Si l'utilisateur souhaite quitter l'ordinateur d'extrémité pendant une courte durée, il peut cliquer sur **Verrouiller le poste de travail** pour empêcher d'autres utilisateurs de l'utiliser et le déverrouiller avec le mot de passe utilisateur. **Non** : l'utilisateur qui a verrouillé l'ordinateur, ainsi qu'un administrateur, peuvent le déverrouiller. Si un administrateur déverrouille l'ordinateur, l'utilisateur connecté est automatiquement déconnecté. **Oui** : change ce comportement. Dans ce cas, seul l'utilisateur peut déverrouiller l'ordinateur. L'administrateur ne pourra pas le déverrouiller et l'utilisateur ne sera pas déconnecté automatiquement.
Activer la présélection utilisateur/domaine	**Oui** : l'authentification au démarrage SafeGuard enregistre le nom et le domaine du dernier utilisateur connecté. Il n'est donc

Paramètre de stratégie	Explication
	pas nécessaire que les utilisateurs saisissent leur nom d'utilisateur chaque fois qu'ils se connectent. **Non** : l'authentification au démarrage SafeGuard n'enregistre pas le nom et le domaine du dernier utilisateur connecté.
Liste de comptes de service	Pour éviter que les opérations d'administration sur un ordinateur protégé par SafeGuard Enterprise n'activent l'authentification au démarrage et n'entraînent l'ajout des opérateurs en charge du déploiement comme autant d'utilisateurs possibles de l'ordinateur, SafeGuard Enterprise vous permet de créer des listes de comptes de service pour la connexion Windows sur les ordinateurs d'extrémité SafeGuard Enterprise. Les utilisateurs de la liste sont traités comme des utilisateurs invités SafeGuard Enterprise. Avant de sélectionner une liste, vous devez créer les listes dans la zone de navigation **Stratégies** sous **Listes de comptes de service**.
Connexion automatique vers Windows	**Remarque :** pour que l'utilisateur puisse autoriser d'autres utilisateurs à accéder à son ordinateur, il doit pouvoir désactiver la connexion automatique vers Windows. ■ **Laisser l'utilisateur choisir** En sélectionnant/dessélectionnant cette option dans la boîte de dialogue de connexion à l'authentification au démarrage SafeGuard, l'utilisateur peut choisir d'exécuter ou non la connexion automatique à Windows. ■ **Désactiver l'authentification automatique à Windows** Après la connexion à l'authentification au démarrage SafeGuard, la boîte de dialogue de connexion Windows s'affiche. L'utilisateur doit se connecter manuellement à Windows. ■ **Appliquer l'authentification automatique à Windows** L'utilisateur se connecte toujours automatiquement à Windows.
OPTIONS BITLOCKER	
Mode de connexion BitLocker	Pour le mode de connexion BitLocker, les options disponibles sont disponibles : ■ **TPM** : la clé de connexion est stockée sur la puce du TPM. ■ **TPM + PIN** : la clé de connexion est stockée sur la puce du TPM et un code PIN est également nécessaire pour la

Paramètre de stratégie	Explication
	connexion. Les paramètres du code PIN sont fournis sous le code PIN et le mot de passe. ■ **Carte mémoire USB** : la clé de connexion est stockée sur une clé USB. ■ **TPM + carte mémoire USB** : la clé de connexion est stockée sur la puce du TPM et sur une clé USB. La connexion peut s'effectuer avec la puce du TPM ou la clé USB. **Remarque :** si vous voulez utiliser **TPM + PIN**, **TPM + Carte mémoire USB** ou **Carte mémoire USB**, veuillez activer la Stratégie de groupe **Authentification supplémentaire requise au démarrage** soit dans Active Directory, soit localement sur les ordinateurs. Dans l'Éditeur d'objets de stratégie de groupe (gpedit.msc), la Stratégie de groupe se trouve à l'emplacement suivant : Stratégie de l'ordinateur local\Configuration ordinateur\Modèles d'administration\Composants Windows\Chiffrement de lecteur BitLocker\Lecteur du système d'exploitation. Pour utiliser la méthode **Carte mémoire USB**, veuillez également activer **Autoriser BitLocker sans un module de plateforme sécurisée compatible** dans la Stratégie de groupe.
Mode de connexion de secours BitLocker	En cas d'échec de connexion, SafeGuard Enterprise permet la connexion avec une clé USB comme mécanisme de secours ou génère un message d'erreur. **Remarque :** si vous sélectionnez **Carte mémoire USB** comme mode de connexion, cette option n'est pas proposée.
ÉCHECS DE CONNEXION	
Nbre maximum d'échecs de connexion	Détermine le nombre de tentatives de connexion d'un utilisateur avec un nom d'utilisateur ou un mot de passe non valide. Par exemple, après trois tentatives successives de saisie d'un nom d'utilisateur ou d'un mot de passe incorrect, une quatrième tentative verrouille l'ordinateur.
Messages d'échec de connexion dans la POA	Définit le niveau de détail des messages d'échec de connexion: ■ **Standard** : affiche une brève description. ■ **Détaillé** : affiche des informations plus détaillées.
OPTIONS DE CARTE À PUCE	

Paramètre de stratégie	Explication
Action si l'état de connexion à la carte à puce est perdu	Définit le comportement après suppression du token de l'ordinateur : Les actions possibles sont les suivantes : ■ **Verrouiller l'ordinateur** ■ **Présenter la boîte de dialogue PIN** ■ **Aucune action**
Autoriser le déblocage de la carte à puce	Détermine si le token peut être débloqué lors de la connexion.
OPTIONS DE VERROUILLAGE	
Verrouiller l'écran après X minutes d'inactivité	Détermine le délai à l'issue duquel un bureau inutilisé est automatiquement verrouillé. La valeur par défaut est de 0 minute, auquel cas le bureau n'est pas verrouillé.
Verrouiller l'écran au retrait de la carte à puce	Détermine si l'écran est verrouillé lorsqu'un token est retiré au cours d'une session.
Verrouiller l'écran après mise en veille	Détermine si l'écran est verrouillé quand l'ordinateur est réactivé du mode veille.

17.3 Création de listes de codes PIN interdits à utiliser dans les stratégies

Pour les stratégies de type **PIN**, une liste de codes PIN interdits peut être créée afin de définir quelles sont les séquences de caractères à ne pas utiliser dans les codes PIN. Les codes PIN sont utilisés pour la connexion avec le token. Retrouvez plus d'informations à la section Tokens et cartes à puce à la page 198.

Les fichiers texte contenant les informations requises doivent être créés avant de pouvoir les enregistrer dans le SafeGuard Management Center. La taille maximale de ces fichiers texte est de **50 Ko**. SafeGuard Enterprise utilise les textes codés en Unicode UTF-16 uniquement. Si vous créez les fichiers texte dans un autre format, ils seront automatiquement convertis lorsqu'ils seront enregistrés.

Remarque : dans les listes, les codes PIN interdits sont séparés par un saut de ligne.

Pour enregistrer les fichiers texte :

1. Dans la zone de navigation de stratégie, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau** > **Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.

3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque : grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

17.4 Règles de syntaxe des codes PIN

Dans les stratégies du type **Code PIN**, vous définissez les paramètres des codes PIN du token.

Les codes PIN peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau code PIN, n'utilisez pas de caractère avec la combinaison ALT + <caractère> car ce mode de saisie n'est pas disponible dans l'authentification au démarrage SafeGuard.

Remarque : définissez des règles de code PIN dans SafeGuard Management Center ou dans Active Directory, mais pas dans les deux.

Paramètre de stratégie	Explication
PIN	
Longueur minimum du code PIN	Spécifie le nombre de caractères que doit contenir un code PIN lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des boutons en forme de flèche.
Longueur max. du code PIN	Spécifie le nombre maximum de caractères que peut contenir un code PIN lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des boutons en forme de flèche.
Nombre min. de lettres **Nombre min. de chiffres** **Nombre min. de caractères spéciaux**	Ces paramètres spécifient qu'un code PIN ne doit pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais une combinaison de ces 2 au moins (par exemple, 15fleur, etc.). Ces paramètres ne sont pratiques que si vous avez défini une longueur minimum de code PIN supérieure à 2.
Respecter la casse	Ce paramètre ne s'applique qu'avec **Utiliser la liste des codes PIN interdits** et **Utilisation interdite du nom d'utilisateur comme code PIN**. **Exemple 1 :** vous avez saisi "tableau" dans la liste des codes PIN interdits. Si l'option **Respecter la casse** est définie sur **OUI**, les

Paramètre de stratégie	Explication
	variantes supplémentaires du code PIN telles que TABLEAU, TablEAU ne seront pas acceptées et la connexion sera refusée. **Exemple 2 :** "EMaier" est saisi comme nom d'utilisateur. Si l'option **Respecter la casse** est définie sur **Oui** et si l'option **Utilisation interdite du nom d'utilisateur en tant que code PIN** est définie sur **Non**, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple, "emaier" ou "eMaiER") comme code PIN.
Interdire la succession de touches horizontales	"123" et "aze" sont des exemples de séquences de touches consécutives. Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire la succession de touches verticales	Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple "wqa1", "xsz2" ou "3edc" (mais pas "wse4", "xdr5" ou "cft6"). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme codes PIN. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Au moins 3 caractères consécutifs non autorisés	L'activation de cette option interdit les séquences de touches ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant ("abc" ; "cba" ; ";", etc.). ■ constituées de trois symboles identiques ou plus ("aaa" ou "111").
Utilisation interdite du nom d'utilisateur comme code PIN	Détermine si le nom d'utilisateur et le code PIN peuvent être identiques. **Oui** : le nom d'utilisateur Windows et le code PIN doivent être différents. **Non** : l'utilisateur peut utiliser son nom d'utilisateur Windows comme code PIN.
Utiliser la liste des codes PIN interdits	Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les codes PIN. Les séquences de caractères sont stockées dans la **Liste de codes PIN non autorisés** (par exemple, un fichier .txt).
Liste de PIN non autorisés	Définit les séquences de caractères à ne pas utiliser pour les codes PIN. Si un utilisateur utilise un code PIN non autorisé, un message d'erreur s'affiche. **Condition préalable :** Une liste (fichier) de codes PIN non autorisés doit être enregistrée dans le Management Center, dans la zone de navigation de stratégie

Paramètre de stratégie	Explication
	sous **Texte d'informations**. La liste n'est disponible qu'après l'enregistrement. Taille de fichier maximale : 50 Ko Format pris en charge : Unicode **Définition des codes PIN interdits** Dans la liste, les codes PIN non autorisés sont séparés par un espace ou un saut de ligne. *Caractère générique :* Le caractère générique "*" peut représenter tout caractère et tout nombre de caractères dans un code PIN. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme code PIN. **Remarque :** ■ Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. ■ Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier. ■ L'option **Utiliser la liste des codes PIN interdits** doit être activée.
MODIFICATIONS	
Modification du code PIN après un min. de (jours)	Détermine la période pendant laquelle un code PIN ne peut pas être modifié. Ce paramètre empêche l'utilisateur de changer trop souvent de code PIN au cours d'une période donnée. **Exemple :** L'utilisateur Bertrand définit un nouveau code PIN (par exemple, "13jk56"). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de changer le code PIN par "13jk56". Le changement de code PIN est refusé car Monsieur Bertrand ne peut définir un nouveau code PIN qu'après un délai de cinq jours.
Changement de code PIN après un max. de (jours)	Si la période de validité maximum est activée, l'utilisateur doit définir un nouveau code PIN une fois la période définie expirée.
Avertir d'un changement obligatoire avant (jours)	Un message d'avertissement s'affiche "n" jours avant l'expiration du code PIN pour rappeler à l'utilisateur de changer son code PIN dans "n" jours. L'utilisateur peut également le changer immédiatement.
GÉNÉRAL	
Masquer les entrées	Indique si les entrées sont masquées lors de la saisie des codes PIN.

Paramètre de stratégie	Explication
Longueur de l'historique du code PIN	Détermine à quel moment des codes PIN déjà utilisés peuvent l'être à nouveau. Il est judicieux de définir la longueur d'historique conjointement au paramètre **Changer de code PIN après un max. de (jours)**. **Exemple :** La longueur d'historique du code PIN pour l'utilisateur Bertrand est définie à 4 et le nombre de jours à l'issue desquels l'utilisateur doit changer son code PIN est de 30. M.Bertrand se connecte actuellement en utilisant le code PIN « Informatique ». Lorsque la période de 30 jours expire, il est invité à changer son code PIN. M. Bertrand saisit "Informatique" comme nouveau code PIN et reçoit un message d'erreur indiquant que ce code PIN a déjà été utilisé et qu'il doit en sélectionner un nouveau. M. Bertrand ne peut pas utiliser le code PIN "Informatique" avant la quatrième invitation de changement du code PIN (en d'autres termes, longueur d'historique du code PIN = 4).

17.5 Création d'une liste de mots de passe interdits à utiliser dans les stratégies

Pour les stratégies de type **Mot de passe**, une liste de mots de passe peut être créée afin de définir quelles sont les séquences de caractères qui ne doivent pas être utilisées dans les mots de passe.

Remarque : dans les listes, les mots de passe non autorisés sont séparés par un saut de ligne.

Les fichiers texte contenant les informations requises doivent être créés avant de pouvoir les enregistrer dans le SafeGuard Management Center. La taille maximale de ces fichiers texte est de **50 Ko**. Sophos SafeGuard utilise les textes codés en Unicode UTF-16 uniquement. Si vous créez les fichiers texte dans un autre format, ils seront automatiquement convertis lorsqu'ils seront enregistrés.

Si un fichier est converti, un message apparaît.

Pour enregistrer des fichiers texte :

1. Dans la zone de navigation de stratégie, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau** > **Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque : grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

17.6 Règles de syntaxe des mots de passe

Les mots de passe peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau mot de passe, n'utilisez pas de caractère avec la combinaison ALT + <caractère> car ce mode de saisie n'est pas disponible dans l'authentification au démarrage SafeGuard. Les règles relatives aux mots de passe utilisés pour se connecter au système sont définies dans des stratégies du type **Mot de passe**.

Remarque : retrouvez plus d'informations sur l'application d'une stratégie de mot de passe fort à la section Bon usage en matière de sécurité à la page 6 ainsi que dans le *Manuel SafeGuard Enterprise pour une utilisation conforme à la certification*.

L'application de règles de mots de passe et l'historique des mots de passe peuvent seulement être garantis si le fournisseur de codes d'accès SGN est utilisé en permanence. Définissez des règles de mots de passe soit dans le SafeGuard Management Center, soit dans Active Directory, pas dans les deux.

Paramètre de stratégie	Explication
Mot de passe	
Longueur minimum du mot de passe	Spécifie le nombre de caractères que doit contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des boutons en forme de flèche.
Longueur max. du mot de passe	Spécifie le nombre maximum de caractères que peut contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des boutons en forme de flèche.
Nombre min. de lettres **Nombre min. de chiffres** **Nombre min. de caractères spéciaux**	Ces paramètres spécifient qu'un mot de passe ne doit pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais une combinaison de ces 2 au moins (par exemple, 15fleur, etc.). Ces paramètres ne sont pratiques que si vous avez défini une longueur minimum de mot de passe supérieure à 2.
Respecter la casse	Ce paramètre ne s'applique qu'avec **Utiliser la liste des mots de passe interdits** et **Utilisation interdite du nom d'utilisateur comme mot de passe**. **Exemple 1 :** vous avez saisi "tableau" dans la liste des mots de passe interdits. Si l'option **Respecter la casse** est définie sur **Oui**, les variantes supplémentaires du mot de passe telles que TABLEAU, TablEAU ne seront pas acceptées et la connexion sera refusée.

Paramètre de stratégie	Explication
	Exemple 2 : "EMaier" est saisi comme nom d'utilisateur. Si l'option **Respecter la casse** est définie sur **Oui** et si l'option **Utilisation interdite du nom d'utilisateur en tant que mot de passe** est définie sur **Non**, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple, "emaier" ou "eMaiER") comme mot de passe.
Interdire la succession de touches horizontales	"123" et "aze" sont des exemples de séquences de touches consécutives. Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire la succession de touches verticales	Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple "wqa1", "xsz2" ou "3edc" (mais pas "wse4", "xdr5" ou "cft6"). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mot de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Au moins 3 caractères consécutifs non autorisés	L'activation de cette option interdit les séquences de touches ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant ("abc" ; "cba" ; ";", etc.). ■ constituées de trois symboles identiques ou plus ("aaa" ou "111").
Utilisation interdite du nom d'utilisateur comme mot de passe	Détermine si le nom d'utilisateur et le mot de passe peuvent être identiques. **Oui** : le nom d'utilisateur Windows et le mot de passe doivent être différents. **Non** : l'utilisateur peut utiliser son nom d'utilisateur Windows comme mot de passe.
Utiliser la liste de mots de passe interdits	Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les mots de passe. Les séquences de caractères sont stockées dans la **Liste des mots de passe interdits** (par exemple, un fichier .txt).
Liste de mots de passe interdits	Définit les séquences de caractères à ne pas utiliser pour les mots de passe. Si un utilisateur utilise un mot de passe non autorisé, un message d'erreur s'affiche. Une liste (fichier) de mots de passe non autorisés doit être enregistrée dans le SafeGuard Management Center, dans la zone de navigation des stratégies sous **Texte d'informations**. La liste n'est disponible qu'après l'enregistrement. Taille de fichier maximale : 50 Ko

Paramètre de stratégie	Explication
	Format pris en charge : Unicode **Définition de mots de passe interdits** Dans la liste, les mots de passe non autorisés sont séparés par un saut de ligne. *Caractère générique* : Le caractère générique « * » peut représenter tout caractère et tout nombre de caractères dans un mot de passe. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme mot de passe. **Remarque :** ■ Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. ■ Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier. ■ L'option **Utiliser la liste des mots de passe interdits** doit être activée.
Synchronisation du mot de passe de l'utilisateur avec les autres clients SGN	Ce champ détermine la procédure de synchronisation des mots de passe lorsque des utilisateurs utilisant plusieurs ordinateurs d'extrémité utilisateur SafeGuard Enterprise, et définis comme les utilisateurs de ces ordinateurs, changent leurs mots de passe. Les options suivantes sont disponibles : ■ Lent (attendre que l'utilisateur se connecte) Si un utilisateur change son mot de passe sur un ordinateur d'extrémité SafeGuard Enterprise et s'il tente de se connecter à un autre ordinateur sur lequel il est également enregistré, il doit tout d'abord se connecter avec son ancien mot de passe à l'authentification au démarrage. La synchronisation du mot de passe n'est effectuée qu'après la connexion avec l'ancien mot de passe. ■ Rapide (attendre la connexion de la machine) Si un utilisateur change son mot de passe sur un ordinateur d'extrémité SafeGuard Enterprise, la synchronisation du mot de passe avec d'autres ordinateurs, sur lesquels l'utilisateur est également enregistré, est effectuée dès que l'autre ordinateur a établi une connexion avec le serveur. C'est le cas, par exemple, lorsqu'un autre utilisateur, également enregistré en tant qu'utilisateur de l'ordinateur, se connecte simultanément à l'ordinateur.
MODIFICATIONS	
Modification du mot de passe autorisée après un min. de (jours)	Détermine la période pendant laquelle un mot de passe ne peut être modifié. Ce paramètre empêche l'utilisateur de changer trop souvent de mot de passe au cours d'une période donnée.

Paramètre de stratégie	Explication
	Si l'utilisateur est forcé à changer son mot de passe par Windows ou s'il modifie son mot de passe après l'affichage du message d'avertissement indiquant que le mot de passe expirera dans X jours, ce paramètre ne sera pas évalué. **Exemple :** L'utilisateur Bertrand définit un nouveau mot de passe (par exemple, "13jk56"). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de changer le mot de passe en "13jk56". Le changement de mot de passe est refusé car l'utilisateur Bertrand ne peut définir un nouveau mot de passe qu'après un délai de cinq jours.
Expiration du mot de passe après (jours)	Si la période de validité maximum est activée, l'utilisateur doit définir un nouveau mot de passe une fois la période définie expirée.
Avertir d'un changement obligatoire avant (jours)	Un message d'avertissement s'affiche «n» jours avant l'expiration du mot de passe pour rappeler à l'utilisateur de changer son mot de passe dans «n» jours. L'utilisateur peut également le changer immédiatement.
GÉNÉRAL	
Masquer les entrées	Indique si les entrées sont masquées lors de la saisie des mots de passe.
Longueur de l'historique de mot de passe	Détermine à quel moment des mots de passe déjà utilisés peuvent l'être à nouveau. Il est judicieux de définir la longueur d'historique conjointement au paramètre **Expiration du mot de passe après (jours)**. **Exemple :** La longueur d'historique du mot de passe pour l'utilisateur Bertrand est définie à 4 et le nombre de jours à l'issue desquels l'utilisateur doit changer son mot de passe est de 30. M.Bertrand se connecte actuellement en utilisant le mot de passe « Informatique ». Lorsque la période de 30 jours expire, il est invité à modifier son mot de passe. M. Bertrand saisit « Informatique » comme nouveau mot de passe et reçoit un message d'erreur indiquant que ce mot de passe a déjà été utilisé et qu'il doit en sélectionner un nouveau. M. Bertrand ne peut pas utiliser le mot de passe « Informatique » avant la quatrième invitation de changement du mot de passe (en d'autres termes, longueur d'historique du mot de passe = 4).

17.7 Phrase secrète pour SafeGuard Data Exchange

L'utilisateur doit entrer une phrase secrète qui est utilisée pour générer des clés locales pour un échange sécurisé des données avec SafeGuard Data Exchange. Les clés générées sur les

ordinateurs d'extrémité sont également stockées dans la base de données SafeGuard Enterprise. Dans les stratégies du type **Phrase secrète**, vous définissez les conditions requises correspondantes.

Retrouvez une description de SafeGuard Data Exchange à la section SafeGuard Data Exchange à la page 177.

Retrouvez plus d'informations sur SafeGuard Data Exchange et sur SafeGuard Portable sur l'ordinateur d'extrémité dans le *Manuel d'utilisation de SafeGuard Enterprise*, au chapitre *SafeGuard Data Exchange*.

Paramètre de stratégie	Explication
PHRASE SECRÈTE	
Longueur minimum de la phrase secrète	Définit le nombre minimum de caractères de la phrase secrète à partir de laquelle la clé est générée. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Longueur max. de la phrase secrète	Définit le nombre maximum de caractères de la phrase secrète. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Nombre min. de lettres **Nombre min. de chiffres** **Nombre min. de caractères spéciaux**	Ce paramètre spécifie qu'une phrase secrète ne peut pas contenir seulement des lettres, des nombres ou des symboles mais doit comporter une combinaison de ces 2 au moins (par exemple, 15 fleur etc.). Ce paramètre n'est pratique que si vous avez défini une longueur minimum de phrase secrète supérieure à 2.
Respecter la casse	Ce paramètre est effectif lorsque l'option **Utilisation interdite du nom d'utilisateur en tant que phrase secrète** est active. **Exemple :** "EMaier" est saisi comme nom d'utilisateur. Si l'option **Respecter la casse** est définie sur OUI et si **Utilisation interdite du nom d'utilisateur en tant que phrase secrète** est définie sur NON, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple emaier ou eMaiER) comme phrase secrète.
Interdire la succession de touches horizontales	Les séquences de touches consécutives sont, par exemple "123" ou "aze". Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire la succession de touches verticales	Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple "wqa1", "xsz2" ou "3edc" (mais pas "wse4", "xdr5" ou "cft6"). Un maximum de deux caractères adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mots de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.

Paramètre de stratégie	Explication
Au moins 3 caractères consécutifs non autorisés	L'activation de cette option interdit les séquences de touches ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant ("abc" ; "cba" ; ";", etc.). ■ constituées de trois symboles identiques ou plus ("aaa" ou "111").
Utilisation interdite du nom d'utilisateur comme phrase secrète	Détermine si le nom d'utilisateur et la phrase secrète peuvent être identiques. **Oui** : le nom d'utilisateur Windows et la phrase secrète doivent être différents. **Non** : l'utilisateur peut utiliser son nom d'utilisateur Windows comme phrase secrète.

17.8 Listes blanches pour les stratégies de protection des périphériques pour le chiffrement basé sur fichier

Dans le SafeGuard Management Center, vous pouvez sélectionner des listes blanches comme cibles pour les stratégies du type **Protection des périphériques** pour le chiffrement basé sur fichier. Ceci vous permet de créer des stratégies de chiffrement pour des modèles de périphériques spécifiques ou même pour des périphériques distincts.

Avant de sélectionner une liste blanche comme cible pour une stratégie **Protection des périphériques**, vous devez la créer et l'enregistrer dans le SafeGuard Management Center. Vous pouvez définir des listes blanches pour des modèles de périphériques de stockage spécifiques (par exemple, un iPod, des périphériques USB provenant d'un fournisseur particulier, etc.) ou pour des périphériques de stockage distincts en fonction du numéro de série. Vous pouvez ajouter manuellement les périphériques aux listes blanches ou utiliser les résultats d'un contrôle SafeGuard PortAuditor. Retrouvez plus d'informations dans le *Guide d'utilisation de SafeGuard PortAuditor*.

Ensuite, vous pouvez sélectionner la liste blanche en tant que cible lorsque vous créez la stratégie de **Protection des périphériques**.

Remarque : si vous sélectionnez une liste blanche comme cible pour une stratégie du type **Protection des périphériques**, vous pouvez seulement sélectionner **Basé sur fichier** ou **Aucun chiffrement** comme **Mode de chiffrement du support**. Si vous sélectionnez **Aucun chiffrement** pour une stratégie **Protection des périphériques** avec une liste blanche, cette stratégie n'exclut aucun périphérique du chiffrement, si une autre stratégie est appliquée qui spécifie le chiffrement basé sur volume.

Remarque : concernant les périphériques SafeStick de BlockMaster, des conditions requises particulières s'appliquent. Ces périphériques ont des identifications différentes pour les administrateurs et les utilisateurs sans droits administrateur. Pour une gestion cohérente dans SafeGuard Enterprise, vous devez ajouter les deux identifications aux listes blanches. SafeGuard

Port Auditor détecte les deux identifications, si un périphérique SafeStick a été ouvert au moins une fois sur l'ordinateur contrôlé par SafeGuard Port Auditor.

17.8.1 Création de listes blanches pour les stratégies de protection des périphériques pour le chiffrement basé sur fichier

1. Dans la zone de navigation **Stratégies**, sélectionnez **Liste blanche**.
2. Dans le menu contextuel **Liste blanche**, cliquez sur **Nouveau** > **Liste blanche**.
3. Sélectionnez le type de liste blanche :
    - Pour créer une liste blanche pour des modèles de périphériques spécifiques, sélectionnez **Modèles de périphériques de stockage**.
    - Pour créer une liste blanche pour des périphériques spécifiques en fonction du numéro de série, sélectionnez **Périphériques de stockage distincts**.
4. Sous **Source de liste blanche**, spécifiez comment vous voulez créer la liste blanche :
    - Pour saisir manuellement les périphériques, sélectionnez **Créer manuellement une liste blanche**.

      Lorsque vous cliquez sur **OK**, une liste blanche vide s'ouvre dans le SafeGuard Management Center. Dans cette liste blanche vide, vous pouvez créer manuellement des entrées. Pour ajouter une nouvelle entrée, cliquez sur l'icône verte **Ajouter** (**Insérer**) dans la barre d'outils du SafeGuard Management Center.

      Remarque : pour récupérer les chaînes correspondantes d'un périphérique dans le Gestionnaire de périphériques Windows, ouvrez la fenêtre **Propriétés** du périphérique et observez les valeurs des propriétés **Numéros d'identification du matériel** et **Chemin d'accès à l'instance du périphérique**. Seules les interfaces suivantes sont prises en charge : USB, 1394, PCMCIA et PCI.
    - Si vous voulez utiliser le résultat d'un contrôle des ordinateurs d'extrémité par SafeGuard PortAuditor comme source, sélectionnez **Importer le résultat de SafeGuard Port Auditor**.

      Les résultats de l'analyse SafeGuard Port Auditor doivent être disponibles (fichier XML) si vous voulez créer la liste blanche avec cette source. Pour sélectionner le fichier, cliquez sur le bouton [**...**].

      Retrouvez plus d'informations dans le *Guide d'utilisation de SafeGuard PortAuditor*.

      Cliquez sur **OK** pour afficher le contenu du fichier importé dans le SafeGuard Management Center.

La liste blanche apparaît sous **Listes blanches** dans la zone de navigation **Stratégies**. Vous pouvez la sélectionner lorsque vous créez des stratégies du type **Protection des périphériques** pour le chiffrement basé sur fichier.

17.8.2 Sélection de listes blanches comme cibles des stratégies de protection des périphériques pour le chiffrement basé sur fichier

Condition préalable : La liste blanche requise doit avoir été créée dans le SafeGuard Management Center.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis sélectionnez **Nouveau**.
3. Sélectionnez **Protection des périphériques**.

   Une boîte de dialogue permettant de nommer la nouvelle stratégie s'affiche.

4. Saisissez un nom et éventuellement une description de la nouvelle stratégie.
5. Sous **Cible de protection de périphérique**, sélectionnez la liste blanche correspondante :
   - Si vous avez créé une liste blanche pour les modèles de périphériques de stockage, elle apparaît sous **Modèles de périphériques de stockage**.
   - Si vous avez créé une liste blanche pour les périphériques de stockage distincts, elle apparaît sous **Périphériques de stockage distincts**.
6. Cliquez sur **OK**.

La liste blanche a été sélectionnée comme cible pour la stratégie de **Protection des périphériques**. Une fois que la stratégie a été transférée sur l'ordinateur d'extrémité, le mode de chiffrement sélectionné dans la stratégie s'applique.

17.9 Protection des périphériques

Les stratégies du type **Protection du périphérique** couvrent les paramètres pour le chiffrement des données sur différents périphériques de stockage des données. Le chiffrement peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents. Les stratégies de type **Protection du périphérique** incluent également des paramètres pour SafeGuard Data Exchange, SafeGuard Cloud Storage et SafeGuard Portable. Retrouvez plus d'informations sur SafeGuard Data Exchange à la section SafeGuard Data Exchange à la page 177. Retrouvez plus d'informations sur SafeGuard Cloud Storage à la section Cloud Storage à la page 187. Retrouvez plus d'informations sur SafeGuard Data Exchange, SafeGuard Cloud Storage et SafeGuard Portable sur l'ordinateur d'extrémité dans le*Manuel d'utilisation de SafeGuard Enterprise*.

Lors de la création d'une stratégie de protection des périphériques, vous devez d'abord spécifier la cible de la protection du périphérique. Les cibles possibles sont les suivantes :

- Stockage de masse (volumes d'initialisation/autres volumes)
- Supports amovibles
- Lecteurs optiques
- Modèles de périphériques de stockage
- Périphériques de stockage distincts

- Définitions Cloud Storage

Pour chaque cible, créez une stratégie distincte.

Remarque : supports amovibles cibles : une stratégie qui spécifie le chiffrement basé sur volume des lecteurs amovibles et qui permet à l'utilisateur de choisir une clé dans une liste (par exemple, **Toute clé du jeu de clés utilisateur**) peut être contournée par l'utilisateur en ne choisissant aucune clé. Pour s'assurer que les lecteurs amovibles sont toujours chiffrés, utilisez une stratégie de chiffrement basée sur fichier ou définissez explicitement une clé dans la stratégie de chiffrement basée sur volume.

Paramètre de stratégie	Explication
Mode de chiffrement du support	Permet de protéger les périphériques (PC, ordinateurs portables, etc.) ainsi que tous types de supports amovibles. **Remarque :** ce paramètre est obligatoire. L'objectif essentiel consiste à chiffrer toutes les données stockées sur des périphériques de stockage locaux ou externes. La méthode de fonctionnement transparente permet aux utilisateurs de continuer à utiliser leurs applications courantes, par exemple Microsoft Office. Le chiffrement transparent signifie que toutes les données chiffrées (dans des répertoires ou dans des volumes chiffrés) sont automatiquement déchiffrées dans la mémoire principale dès qu'elles sont ouvertes dans un programme. Un fichier est automatiquement chiffré de nouveau lorsqu'il est enregistré. Les options suivantes sont disponibles : ■ **Aucun chiffrement** ■ **Basé sur volume** (= chiffrement transparent basé sur secteur) Garantit que toutes les données sont chiffrées (y compris les fichiers d'initialisation, les fichiers d'échange, les fichiers inactifs/d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sans que l'utilisateur ait à modifier ses habitudes de travail ou tenir compte de problèmes de sécurité. ■ **Basé sur fichier** (= chiffrement transparent basé sur fichier, Chiffrement Smart Media) Garantit que toutes les données sont chiffrées (à l'exception du support d'initialisation et des informations de répertoire) avec l'avantage que même les supports optiques tels que les CD/DVD peuvent être chiffrés et que les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard Enterprise n'est pas installé (si les stratégies l'autorisent). **Remarque :** pour les stratégies avec listes blanches, seuls **Aucun chiffrement** ou **Basé sur fichier** peuvent être sélectionnés.
PARAMÈTRES GÉNÉRAUX	

Paramètre de stratégie	Explication
Algorithme à utiliser pour le chiffrement	Définit l'algorithme de chiffrement. Liste des algorithmes utilisables avec les normes respectives : AES256 : 32 octets (256 bits) AES128 : 16 octets (128 bits)
Clé à utiliser pour le chiffrement	Définit la clé utilisée pour le chiffrement. Vous pouvez définir des clés spécifiques (clé machine ou une clé définie par ex.) ou vous pouvez autoriser l'utilisateur à sélectionner une clé. Vous pouvez également limiter les clés qu'un utilisateur est autorisé à utiliser. Les options suivantes sont disponibles : ■ **Toute clé du jeu de clés utilisateur** Toutes les clés du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. **Remarque :** cette option doit être sélectionnée si vous définissez une stratégie de chiffrement basé sur fichier pour un ordinateur d'extrémité non administré protégé par SafeGuard Enterprise (autonome). ■ **Toute clé du jeu de clés utilisateur sauf la clé utilisateur** Toutes les clés sauf celles du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. ■ **Toute clé de groupe du jeu de clés utilisateur** Toutes les clés de groupe du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. ■ **Clé machine définie** La clé de la machine est utilisée, l'utilisateur ne peut PAS sélectionner de clé. **Remarque :** cette option doit être sélectionnée si vous définissez une stratégie de chiffrement basé sur volume pour un ordinateur d'extrémité non administré protégé par SafeGuard Enterprise (mode autonome). Si vous sélectionnez néanmoins **Toute clé du jeu de clés utilisateur** et si l'utilisateur sélectionne une clé créée localement pour le chiffrement basé sur volume, l'accès à ce volume sera refusé. ■ **Toute clé du jeu de clés utilisateur sauf les clés créées localement** Toutes les clés sauf les clés générées localement à partir d'un jeu de clés sont affichées et l'utilisateur peut sélectionner l'une d'entre elles. ■ **Clé définie dans la liste**

Paramètre de stratégie	Explication
	L'administrateur peut sélectionner n'importe quelle clé disponible lorsqu'il définit des stratégies dans le Management Center.
	La clé doit être sélectionnée sous **Clé définie pour le chiffrement**. **Si l'option Clé machine définie est utilisée :** Si SafeGuard Data Exchange est uniquement installé sur l'ordinateur d'extrémité (pas d'authentification au démarrage SafeGuard, ni de chiffrement basé sur volume), une stratégie définissant la **Clé machine définie** comme étant la clé à utiliser pour le chiffrement basé sur fichier ne s'appliquera pas sur cet ordinateur. La clé machine définie n'est pas disponible sur un ordinateur de ce type. Les données ne peuvent pas être chiffrées. Stratégies pour l'ordinateur d'extrémité non administré protégé par SafeGuard Enterprise (autonome) : **Remarque :** notez que seule l'option **Toute clé du jeu de clés utilisateur** peut être utilisée lors de la création de stratégies pour des ordinateurs d'extrémité non administrés. La création de clés locales doit en outre être autorisée pour ce type d'ordinateur d'extrémité. Si la fonction de phrase secrète des supports est activée pour des ordinateurs d'extrémité non administrés, la clé de chiffrement de support est utilisée automatiquement comme **Clé définie pour le chiffrement**. en effet, aucune clé de groupe n'est disponible sur les ordinateurs d'extrémité non administrés. La sélection d'une autre clé sous **Clé définie pour le chiffrement** lors de la création d'une stratégie de support amovible pour des clients autonomes n'a aucun effet.
Clé définie pour le chiffrement	Ce champ ne devient actif que si vous avez sélectionné l'option **Clé définie dans la liste** dans le champ **Clé à utiliser pour le chiffrement**. Cliquez sur **[...]** pour afficher la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour rechercher des clés et en sélectionner une dans la liste qui apparaît. Dans le cas d'une stratégie de type **Protection du périphérique** avec la cible **Supports amovibles**, cette clé sert à chiffrer la clé de chiffrement de support lorsque la fonction de phrase secrète des supports est activée (**L'utilisateur peut définir une phrase secrète des supports pour les périphériques** définie sur **Oui**). Pour des stratégies **Protection des périphériques** pour des supports amovibles, les paramètres ■ **Clé à utiliser pour le chiffrement** ■ **Clé définie pour le chiffrement** doivent donc être spécifiés indépendamment l'un de l'autre.

Paramètre de stratégie	Explication
	Stratégies pour les ordinateurs d'extrémité non administrés protégés par SafeGuard Enterprise (autonome) : Si la fonction de phrase secrète des supports est activée pour des ordinateurs d'extrémité non administrés, la clé de chiffrement de support est utilisée automatiquement comme **Clé définie pour le chiffrement**. en effet, aucune clé de groupe n'est disponible sur les ordinateurs d'extrémité non administrés.
L'utilisateur est autorisé à créer une clé locale	Ce paramètre détermine si les utilisateurs peuvent générer ou non une clé locale sur leurs ordinateurs. Les clés locales sont générées sur l'ordinateur d'extrémité selon une phrase secrète saisie par l'utilisateur. La configuration minimale de la phrase secrète est définie dans des stratégies du type **Phrase secrète**. Ces clés sont également enregistrées dans la base de données. L'utilisateur peut les utiliser sur n'importe quel ordinateur auquel il est connecté. Des clés locales peuvent être utilisées pour l'échange de données sécurisé avec SafeGuard Data Exchange (SG DX).
PARAMÈTRES BASÉS SUR VOLUME	
L'utilisateur peut ajouter des clés au volume chiffré ou en supprimer	**Oui** : les utilisateurs de l'ordinateur d'extrémité peuvent ajouter ou supprimer des clés d'un jeu de clés. La boîte de dialogue s'affiche dans l'onglet **Propriétés/Chiffrement** de la commande du menu contextuel. **Non** : les utilisateurs de l'ordinateur d'extrémité ne peuvent pas ajouter de clés.
Réaction aux volumes non chiffrés	Définit de quelle manière SafeGuard Enterprise gère les supports non chiffrés. Les options suivantes sont disponibles : ■ **Rejeter** (= le support en texte n'est pas chiffré) ■ **Accepter uniquement les supports vierges et chiffrer** ■ **Accepter tous les supports et chiffrer**
L'utilisateur peut déchiffrer le volume	Permet à l'utilisateur de déchiffrer le volume avec une commande du menu contextuel dans l'Explorateur Windows.
Chiffrement initial rapide	Sélectionnez ce paramètre pour activer le mode de chiffrement initial rapide pour le chiffrement basé sur volume. Ce mode réduit le temps nécessaire pour le chiffrement initial sur les ordinateurs d'extrémité. **Remarque :** ce mode peut également entraîner un état plus faible de sécurité. Retrouvez plus d'informations à la section Chiffrement initial rapide à la page 152.

Paramètre de stratégie	Explication
Poursuivre sur les secteurs incorrects	Indique si le chiffrement doit se poursuivre ou être arrêté si des secteurs incorrects sont détectés. Le paramètre par défaut est **Oui**.
PARAMETRES SUR FICHIER	
Chiffrement initial de tous les fichiers	Démarre automatiquement le chiffrement initial d'un volume après la connexion de l'utilisateur. Il se peut que l'utilisateur doive sélectionner une clé du jeu de clés au préalable.
L'utilisateur peut annuler le chiffrement initial.	Permet à l'utilisateur d'annuler le chiffrement initial.
L'utilisateur n'est pas autorisé à accéder aux fichiers non chiffrés	Définit si un utilisateur peut accéder aux données non chiffrées d'un volume.
L'utilisateur peut déchiffrer des fichiers	Permet à un utilisateur de déchiffrer des fichiers individuels ou des répertoires entiers (avec l'extension de l'Explorateur Windows <clic droit>).
L'utilisateur peut définir une phrase secrète des supports pour les périphériques	Permet à l'utilisateur de définir une phrase secrète des supports sur son ordinateur. La phrase secrète des supports permet d'accéder facilement via SafeGuard Portable à toutes les clés locales utilisées sur des ordinateurs sur lesquels SafeGuard Data Exchange n'est pas installé.
Supports amovibles et Cloud Storage seulement : **Copier SG Portable sur la cible**	Si cette option est sélectionnée, SafeGuard Portable est copié sur tous les supports amovibles connectés à l'ordinateur d'extrémité et dans tous les dossiers de synchronisation définis par une définition Cloud Storage pour SafeGuard Cloud Storage dès l'écriture de contenu sur le support ou le dossier chiffré. SafeGuard Portable permet l'échange des données chiffrées avec les supports amovibles ou le stockage dans le Cloud sans que SafeGuard Enterprise ne soit installé sur le destinataire. Le destinataire peut déchiffrer et chiffrer de nouveau les fichiers chiffrés en utilisant SafeGuard Portable et le mot de passe correspondant. Le destinataire peut chiffrer de nouveau les fichiers avec SafeGuard Portable ou utiliser la clé d'origine pour le chiffrement. Il n'est pas nécessaire que SafeGuard Portable soit installé ou copié sur l'ordinateur du destinataire, il peut être utilisé directement à partir du support amovible ou du dossier de synchronisation du stockage dans le Cloud.
Clé de chiffrement initial par défaut	Ce champ propose une boîte de dialogue de sélection d'une clé utilisée pour le chiffrement initial basé sur fichier. Si vous sélectionnez une clé ici, l'utilisateur ne peut pas sélectionner de clé au démarrage du chiffrement initial. Le chiffrement initial démarre sans interaction de l'utilisateur. La clé sélectionnée est toujours utilisée pour le chiffrement initial. **Exemple :**

Paramètre de stratégie	Explication
	Condition préalable : une clé par défaut a été définie pour le chiffrement initial. Le chiffrement initial démarre automatiquement lorsque l'utilisateur connecte un périphérique USB à l'ordinateur. La clé définie est utilisée. L'utilisateur ne doit pas intervenir. Si l'utilisateur souhaite chiffrer de nouveau les fichiers ou enregistrer de nouveaux fichiers sur le périphérique USB, il peut sélectionner la clé de son choix (s'il y est autorisé et si disponible). Si l'utilisateur connecte un autre périphérique USB, la clé définie pour le chiffrement initial est de nouveau utilisée. Cette clé est également utilisée pour tous les processus de chiffrement ultérieurs jusqu'à ce que l'utilisateur sélectionne explicitement une autre clé. **Remarque :** cette option est désactivée lorsque la fonction de phrase secrète de support est activée. La **Clé définie pour le chiffrement** sera utilisée.
Dossier en texte brut	Le dossier spécifié ici sera créé sur tous les supports amovibles, périphériques de stockage de masse et dans le dossier de synchronisation de stockage dans le Cloud. Les fichiers copiés dans ce dossier restent au format brut.
L'utilisateur est autorisé à décider de l'opération de chiffrement	Vous pouvez autoriser l'utilisateur à décider du chiffrement des fichiers sur les supports amovibles et sur les périphériques de stockage de masse. ■ Si vous définissez cette option sur **Oui**, les utilisateurs sont invités à décider si les données doivent être chiffrées. Pour les périphériques de stockage en masse, l'invite apparaît après chaque connexion tandis que pour les supports amovibles, l'invite apparaît lorsqu'ils sont connectés. ■ Si vous définissez cette option sur **Oui, se rappeler du paramètre utilisateur**, les utilisateurs peuvent utiliser l'option **Se rappeler de ce paramètre et ne plus afficher cette boîte de dialogue** pour que leurs choix soient conservés pour le périphérique correspondant. Dans ce cas, la boîte de dialogue ne réapparaîtra pas pour le périphérique correspondant. Si l'utilisateur sélectionne **Non** dans la boîte de dialogue sur l'ordinateur d'extrémité, aucun chiffrement initial ou transparent n'a lieu.

17.10 Paramètres de machine spécifiques : paramètres de base

Paramètres de stratégie	Explication
AUTHENTIFICATION AU DÉMARRAGE (POA)	

Paramètres de stratégie	Explication
Activer l'authentification au démarrage	Définit si l'authentification au démarrage SafeGuard est activée ou désactivée. **Remarque :** pour des raisons de sécurité, nous vous conseillons fortement de conserver l'authentification au démarrage SafeGuard activée. La désactivation de l'authentification au démarrage SafeGuard réduit la sécurité du système de connexion Windows et accroît le risque d'accès non autorisés aux données chiffrées.
Refuser l'accès en cas d'absence de connexion au serveur (jours) (0=pas de vérification)	Refuse la connexion à l'authentification au démarrage SafeGuard si l'ordinateur d'extrémité n'a pas été connecté au serveur pendant une période supérieure à la période définie.
ÉVEIL PAR APPEL RÉSEAU SÉCURISÉ (WOL)	Grâce aux paramètres d'**Éveil par appel réseau sécurisé** (**WOL**), vous pouvez préparer les ordinateurs d'extrémité aux déploiements de logiciels. Si les paramètres d'Éveil par appel réseau sécurisé s'appliquent aux ordinateurs d'extrémité, les paramètres nécessaires (par exemple, la désactivation de l'authentification au démarrage SafeGuard et un intervalle d'éveil par appel réseau) sont transférés directement sur les ordinateurs d'extrémité sur lesquels les paramètres sont analysés. **Remarque :** la désactivation de l'authentification au démarrage SafeGuard (même pour un nombre limité de processus d'initialisation) réduit le niveau de sécurité de votre système. Retrouvez plus d'informations sur l'éveil par appel réseau sécurisé à la section Éveil par appel réseau sécurisé (WOL) à la page 215.
Nombre de connexions automatiques	Définit le nombre de redémarrages lorsque l'authentification au démarrage SafeGuard est inactive pour l'éveil par appel réseau. Ce paramètre remplace temporairement le paramètre **Activer l'authentification au démarrage** jusqu'à ce que le nombre prédéfini de connexions automatiques soit atteint. L'authentification au démarrage SafeGuard est ensuite réactivée. Si vous définissez le nombre de connexions automatiques sur deux et si **Activer l'authentification au démarrage** est actif, l'ordinateur d'extrémité démarre deux fois sans authentification via l'authentification au démarrage SafeGuard. Pour le mode Éveil par appel réseau, nous vous conseillons d'autoriser **trois redémarrages de plus que nécessaire** pour faire face aux problèmes imprévus.
Connexion à Windows autorisée pendant le WOL	Détermine si la connexion Windows est autorisée pendant l'éveil par appel réseau, par exemple pour une mise à jour de logiciel. Ce paramètre est interprété par la POA.

Paramètres de stratégie	Explication
Début de la plage horaire pour le lancement du WOL externe **Fin de la plage horaire pour le lancement du WOL externe**	La date et l'heure peuvent être sélectionnées ou saisies pour le début et la fin de l'éveil par appel réseau (WOL). Format de date : *MM/JJ/AAAA* Format d'heure : *HH:MM* Les combinaisons suivantes de saisie sont possibles : ■ début et fin de l'éveil par appel réseau définis ; ■ fin de l'éveil par appel réseau définie, début ouvert. ■ aucune entrée : aucun intervalle n'a été défini. Pour un déploiement planifié de logiciels, le responsable de la sécurité doit définir la plage de l'éveil par appel réseau de sorte que le script de programmation puisse démarrer suffisamment tôt pour que les ordinateurs d'extrémité aient le temps de démarrer. WOLstart (Début WOL) : le point de départ de l'éveil par appel réseau dans le script de programmation doit se trouver dans l'intervalle défini dans la stratégie. Si aucun intervalle n'est défini, l'éveil par appel réseau n'est pas activé localement sur l'ordinateur d'extrémité protégé par SafeGuard Enterprise. WOLstop (Fin WOL) : cette commande s'effectue quel que soit le point d'extrémité défini pour l'éveil par appel réseau.
ATTRIBUTIONS UTILISATEUR/MACHINE (AUM)	
Interdire la connexion à l'utilisateur invité SGN	Définit si les utilisateurs invités peuvent se connecter à Windows sur l'ordinateur d'extrémité. **Remarque :** les comptes Microsoft sont toujours considérés comme des utilisateurs invités de SafeGuard Enterprise.
Autoriser l'enregistrement de nouveaux utilisateurs SGN pour	Définit qui peut importer un autre utilisateur SGN dans l'authentification au démarrage SafeGuard et/ou AUM (en désactivant la connexion automatique vers le système d'exploitation). **Remarque :** pour les ordinateurs d'extrémité sur lesquels le module Protection des périphériques n'est pas installé, le paramètre **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** doit être défini sur **Tout le monde** s'il est possible d'ajouter plusieurs utilisateurs à l'Attribution utilisateur/machine avec accès à leur trousseau de clés. Autrement, les utilisateurs peuvent uniquement être ajoutés dans SafeGuard Management Center. Ce paramètre est uniquement évalué sur les ordinateurs d'extrémité administrés. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/110659.aspx.

Paramètres de stratégie	Explication
Activer l'enregistrement des utilisateurs Windows de SGN	Définit si les utilisateurs Windows de SGN peuvent être enregistrés sur l'ordinateur d'extrémité. Un utilisateur Windows de SGN n'est pas ajouté à l'authentification au démarrage SafeGuard. En revanche, il dispose d'un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur Sophos SGN. Si vous sélectionnez ce paramètre, tous les utilisateurs, qui seraient autrement devenus des utilisateurs invités, deviennent des utilisateurs Windows de SGN. Les utilisateurs sont ajoutés à l'Attribution utilisateur/machine dès qu'ils se connectent à Windows.
Activer l'attribution utilisateur/machine pour les ordinateurs d'extrémité autonomes	**Remarque :** ce paramètre s'applique uniquement aux ordinateurs d'extrémité non administrés. Définit si les utilisateurs peuvent supprimer les utilisateurs SGN et les utilisateurs Windows de SGN de l'attribution utilisateur/machine. Si vous sélectionnez **Oui**, la commande **Attributions utilisateur/machine** est disponible dans le menu de l'icône de la barre d'état système sur l'ordinateur d'extrémité. Cette commande affiche une liste des utilisateurs pouvant se connecter à l'authentification au démarrage SafeGuard en tant qu'utilisateurs SGN et à Windows en tant qu'utilisateurs Windows de SGN. Dans la boîte de dialogue qui s'affiche, il est possible de retirer des utilisateurs de la liste. Une fois que les utilisateurs SGN ou que les utilisateurs Windows de SGN ont été supprimés, ils ne peuvent plus se connecter à l'authentification au démarrage SafeGuard où à Windows.
Nombre maximal d'utilisateurs Windows de SGN avant nettoyage automatique	**Remarque :** ce paramètre s'applique uniquement aux ordinateurs d'extrémité administrés. Ce paramètre vous permet d'activer le nettoyage automatique des utilisateurs Windows de SafeGuard Enterprise sur les ordinateurs d'extrémité administrés. Dès que le seuil que vous avez fixé est dépassé par un utilisateur Windows de SafeGuard Enterprise, tous les utilisateurs Windows de SafeGuard Enterprise sont supprimés de l'Attribution utilisateur/machine à l'exception du nouveau. La valeur par défaut est de **10**.
OPTIONS D'AFFICHAGE	
Afficher l'identification de la machine	Affiche le nom de l'ordinateur ou un texte défini dans la barre de titre de l'authentification au démarrage SafeGuard. Si les paramètres réseau de Windows incluent le nom de l'ordinateur, ce dernier est automatiquement intégré aux paramètres de base.

Paramètres de stratégie	Explication
Texte d'identification de la machine	Le texte à afficher dans la barre de titre de l'authentification au démarrage SafeGuard. Si vous avez sélectionné **Nom défini** dans le champ **Afficher l'identification de la machine**, vous pouvez saisir le texte dans ce champ de saisie.
Afficher la mention légale	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît avant l'identification dans l'authentification au démarrage SafeGuard. Dans certains pays, la loi exige l'affichage d'une zone de texte ayant un certain contenu. L'utilisateur doit confirmer la zone de texte avant que le système ne continue. Avant de spécifier un texte, ce dernier doit être enregistré en tant qu'élément de texte sous **Texte d'informations** dans la zone de navigation **Stratégies**.
Texte de la mention légale	Le texte à afficher en tant que mention légale. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans **Texte d'informations** dans la zone de navigation **Stratégies**.
Afficher des informations supplémentaires	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît après la mention légale (si elle est activée). Vous pouvez définir si les informations supplémentaires sont affichées : ■ Jamais ■ À chaque démarrage système ■ À chaque connexion Avant de spécifier un texte, ce dernier doit être enregistré en tant qu'élément de texte sous **Texte d'informations** dans la zone de navigation **Stratégies**.
Texte des informations supplémentaires	Le texte à afficher en tant qu'informations supplémentaires. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans **Texte d'informations** dans la zone de navigation **Stratégies**.
Afficher pendant (s)	Dans ce champ, vous pouvez définir la durée (en secondes) pendant laquelle les informations supplémentaires doivent être affichées. Vous pouvez spécifier le nombre de secondes après lesquelles la zone de texte d'informations supplémentaires est fermée

Paramètres de stratégie	Explication
	automatiquement. L'utilisateur peut fermer la zone de texte à tout moment en cliquant sur **OK**.
Activer et afficher l'icône de la barre d'état système	L'icône de la barre d'état système de SafeGuard Enterprise permet à l'utilisateur d'accéder rapidement et facilement à l'ensemble des fonctions de l'ordinateur d'extrémité. En outre, des informations concernant l'état de l'ordinateur d'extrémité (nouvelles stratégies reçues, etc.) peuvent être affichées dans des infobulles. **Oui :** l'icône de la barre d'état système est affichée dans la zone d'information de barre des tâches et l'utilisateur est continuellement informé via l'infobulle concernant l'état de l'ordinateur d'extrémité protégé par SafeGuard Enterprise. **Non :** l'icône de la barre d'état système n'est pas affichée. Aucune information d'état n'est affichée par les infobulles. **Muet :** l'icône de la barre d'état système est affichée dans la zone d'information de barre des tâches mais aucune information d'état n'est affichée via les infobulles.
Afficher les icônes en chevauchement dans l'Explorateur	Définit si des symboles de clé Windows s'affichent pour indiquer l'état de chiffrement des volumes, périphériques, dossiers et fichiers.
Clavier virtuel en POA	Définit si un clavier virtuel peut être affiché sur demande dans la boîte de dialogue de l'authentification au démarrage SafeGuard pour la saisie du mot de passe.
OPTIONS D'INSTALLATION	
Désinstallation autorisée	Détermine si la désinstallation de SafeGuard Enterprise est autorisée sur les ordinateurs client. Lorsque l'option **Désinstallation autorisée** est définie sur **Non**, SafeGuard Enterprise ne peut pas être désinstallé, même par un utilisateur avec les droits administrateur, lorsque ce paramètre est actif au sein d'une stratégie.
Activer la protection antialtération Sophos	Active/désactive la protection antialtération Sophos. Si vous avez autorisé la désinstallation de SafeGuard Enterprise dans le paramètre de stratégie **Désinstallation autorisée**, vous pouvez définir ce paramètre de stratégie sur **Oui**, pour garantir que les tentatives de désinstallation sont vérifiées par la protection antialtération Sophos pour empêcher la suppression accidentelle du logiciel.

Paramètres de stratégie	Explication
	Si la protection antialtération Sophos n'autorise pas la désinstallation, les tentatives de désinstallation seront annulées. Si l'option **Activer la protection antialtération Sophos** est définie sur **Non**, la désinstallation de SafeGuard Enterprise ne sera pas vérifiée ou empêchée par la protection antialtération Sophos. **Remarque :** ce paramètre ne s'applique qu'aux ordinateurs d'extrémité à partir de la version 9.5 de Sophos Endpoint Security and Control.
PARAMÈTRES DU FOURNISSEUR DES CODES D'ACCÈS	
Enveloppement du fournisseur de codes d'accès	Vous pouvez configurer SafeGuard Enterprise pour utiliser un fournisseur de codes d'accès différents de ceux du fournisseur de codes d'accès Windows. Les modèles des fournisseurs de codes d'accès pris en charge peuvent être téléchargés sur le site Web de Sophos. Pour obtenir une liste des modèles de fournisseurs de codes d'accès éprouvés et savoir où les télécharger, veuillez contacter le support Sophos. Vous pouvez importer un modèle et le déployer sur les ordinateurs d'extrémité en utilisant le paramètre de la stratégie **Fournisseur de codes d'accès**. Veuillez cliquer sur **Importer le modèle** et naviguez jusqu'au fichier de modèles. Le modèle importé et son contenu sont affichés dans le champ **Fournisseur de codes d'accès** et défini en tant que stratégie. Pour supprimer un modèle, veuillez cliquer sur **Effacer le modèle**. **Remarque :** veuillez ne pas modifier les fichiers de modèles fournis. Si la structure XML de ces fichiers est modifiée, les paramètres ne seront pas reconnus sur l'ordinateur d'extrémité et le fournisseur de codes d'accès Windows par défaut sera utilisé à la place.
PARAMÈTRES DE PRISE EN CHARGE DU TOKEN	
Nom du module middleware du token	Enregistre le module PKCS#11 d'un token. Les options suivantes sont disponibles : ■ Paramètres PKCS#11 personnalisés... ■ ActiveIdentity ActivClient ■ ActiveIdentity ActivClient (PIV) ■ AET SafeSign Identity Client ■ Aladdin eToken PKI Client

Paramètres de stratégie	Explication
	■ a.sign Client ■ Charismathics Smart Security Interface ■ Estonian ID-Card ■ Gemalto Access Client ■ Gemalto Classic Client ■ Gemalto .NET Card ■ IT Solution trustWare CSP+ ■ Nexus Personal ■ RSA Authentication Client 2.x ■ RSA Smart Card Middleware 3.x ■ Siemens CardOS API ■ T-Systems NetKey 3.0 ■ Unizeto proCertum Si vous sélectionnez **Paramètres PKCS#11 personnalisés...**, les **Paramètres PKCS#11 personnalisés** sont activés. Vous pouvez saisir les noms de module à utiliser : ■ Module PKCS#11 pour Windows ■ Module PKCS#11 pour l'authentification au démarrage SafeGuard **Remarque :** si vous installez le middleware **Nexus Personal** ou **Gemalto .NET Card**, vous allez également devoir ajouter leur chemin d'installation à la variable d'environnement PATH des **Propriétés système** de votre ordinateur. ■ Le chemin d'installation par défaut pour **Gemalto .NET Card**:`C:\Program Files\ Gemalto\PKCS11 for .NET V2 smart cards` ■ Le chemin d'installation par défaut pour **Nexus Personal** : `C:\Program Files\Personal\bin` **Licences :** Sachez que l'utilisation des middlewares respectifs pour le système d'exploitation standard requiert un accord de licence avec le fabricant correspondant. Retrouvez plus d'informations sur la définition des autorisations SQL dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/116585.aspx. Pour les licences Siemens, contactez : Atos IT Solutions and Services GmbH

Paramètres de stratégie	Explication
	Otto-Hahn-Ring 6 D-81739 Muenchen Allemagne
Services en attente de	Ce paramètre permet de résoudre les problèmes de certaines cartes à puce. Notre support fournira les paramètres correspondants requis.

17.11 Journalisation pour les ordinateurs d'extrémité Windows

Les événements SafeGuard Enterprise ne sont pas dans l'Observateur d'événements Windows ou dans la base de données SafeGuard Enterprise. Pour spécifier les événements à journaliser et leur destination, créez une stratégie de type **Journalisation** et sélectionnez les événements souhaités en cliquant dessus.

Vous pouvez sélectionner plusieurs types d'événements, de catégories différentes (par exemple authentification, chiffrement, etc.). Nous vous recommandons de définir une stratégie pour la journalisation et de déterminer quels sont les événements nécessaires, en fonction de vos exigences en matière de rapports et d'audits.

Retrouvez plus d'informations à la section Rapports à la page 254.

18 Chiffrement du disque

Cette version de SafeGuard Enterprise prend en charge Windows 7 et Windows 8 fonctionnant sur des ordinateurs d'extrémité dotés de BIOS ou d'UEFI.

- Pour les plates-formes BIOS, vous pouvez choisir entre le chiffrement intégral du disque SafeGuard Enterprise et le chiffrement BitLocker géré par SafeGuard. La version BIOS est livrée avec le mécanisme de récupération BitLocker original.

  Remarque : si l'authentification au démarrage SafeGuard ou le chiffrement intégral du disque SafeGuard sont mentionnés dans le présent manuel, il font uniquement référence aux ordinateurs d'extrémité Windows 7 avec BIOS.

- Pour les plates-formes UEFI, veuillez utiliser BitLocker géré par SafeGuard Enterprise pour le chiffrement du disque. Pour ces ordinateurs d'extrémité, SafeGuard Enterprise offre des fonctionnalités améliorées de Challenge/Réponse. Retrouvez plus de renseignements sur les versions UEFI prises en charge et sur les limites de la prise en charge du Challenge/Réponse SafeGuard BitLocker dans les Notes de publication disponibles sur http://downloads.sophos.com/readmes/readsgn_61_fra.html.

Remarque : la mention UEFI apparaît de manière explicite à chaque fois qu'elle doit être utilisée.

Le tableau ci-dessous indique quels composants sont disponibles.

	Chiffrement du disque SafeGuard avec authentification au démarrage SafeGuard	Authentification au démarrage SafeGuard avec récupération par Challenge/Réponse	Authentification de préinitialisation BitLocker gérée par SafeGuard	Récupération C/R SafeGuard pour l'authentification de préinitialisation BitLocker
Windows 7 BIOS	OUI	OUI	OUI	
Windows 7 UEFI			OUI	OUI
Windows 8 UEFI			OUI	OUI
Windows 8 BIOS			OUI	

18.1 Chiffrement intégral du disque SafeGuard

La fonction principale de SafeGuard Enterprise est le chiffrement des données sur différents périphériques de stockage de données. Le chiffrement intégral du disque peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents.

Les fichiers sont chiffrés de manière transparente. Lorsque les utilisateurs ouvrent, modifient et enregistrent des fichiers, ils ne sont pas invités à chiffrer ou à déchiffrer.

En tant que responsable de la sécurité, définissez des paramètres de chiffrement dans une stratégie de sécurité du type **Protection des périphériques** : Retrouvez plus d'informations aux sections Utilisation de stratégies à la page 71 et Protection des périphériques à la page 135.

Remarque : la fonctionnalité de chiffrement intégral du disque décrite aux sections suivantes peut uniquement être utilisée avec les systèmes BIOS. Si vous utilisez d'autres systèmes tel que UEFI, veuillez utiliser la fonctionnalité intégrée de Chiffrement de lecteur BitLocker de Windows. Retrouvez plus d'informations à la section Chiffrement de lecteur BitLocker à la page 154.

18.1.1 Chiffrement intégral du disque basé sur volume

Avec le chiffrement intégral du disque basé sur volume, toutes les données présentes sur un volume (y compris les fichiers d'initialisation, les fichiers de pages, les fichiers d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sont chiffrées. Les utilisateurs n'ont pas à changer les procédures de fonctionnement normales ou à penser à la sécurité.

Pour appliquer le chiffrement basé sur volume aux ordinateurs d'extrémité, créez une stratégie du type **Protection des périphériques** et définissez le **Mode de chiffrement du support** sur **Basé sur volume**. Retrouvez plus d'informations à la section Protection des périphériques à la page 135.

Remarque :

- Le chiffrement/déchiffrement basé sur volume n'est pas pris en charge pour les lecteurs sans lettre de lecteur attribuée.
- Si une stratégie de chiffrement existe pour un volume ou un type de volume et si le chiffrement du volume échoue, l'utilisateur n'est pas autorisé à y accéder.
- Les ordinateurs d'extrémité peuvent être éteints et redémarrés lors du chiffrement/déchiffrement.
- Si le déchiffrement est suivi d'une désinstallation, nous conseillons de ne pas suspendre, ni de mettre en veille l'ordinateur d'extrémité lors du déchiffrement.
- Si après le chiffrement d'un volume, une nouvelle stratégie est appliquée à un ordinateur d'extrémité qui autorise le déchiffrement, les conditions suivantes s'appliquent : une fois terminé le chiffrement basé sur volume, l'ordinateur d'extrémité doit être redémarré au moins une fois avant que le déchiffrement puisse être lancé.

18.1.1.1 Chiffrement initial rapide

SafeGuard Enterprise propose un chiffrement initial en guise de mode spécial pour le chiffrement basé sur volume. Il réduit le temps nécessaire au chiffrement initial (ou au déchiffrement final) des volumes sur les ordinateurs d'extrémité en accédant uniquement à l'espace disque réellement en cours d'utilisation.

Pour un chiffrement initial rapide, les conditions préalables suivantes s'appliquent :

- Le chiffrement initial rapide fonctionne seulement sur les volumes formatés NTFS.
- Les volumes formatés NTFS avec une taille de clusters de 64 Ko ne peuvent pas être chiffrés avec le mode de chiffrement initial rapide.

Remarque : ce mode conduit à un état moins sécurisé si un disque a été utilisé avant son utilisation courante avec SafeGuard Enterprise. Les secteurs non utilisés peuvent tout de même contenir des données. Le chiffrement initial rapide est par conséquent désactivé par défaut.

Pour activer le chiffrement initial rapide, sélectionnez le paramètre **Chiffrement initial rapide** dans une stratégie du type **Protection des périphériques**.

Remarque : pour le déchiffrement des volumes, le mode de chiffrement initial rapide sera toujours utilisé, quel que soit le paramètre de stratégie spécifié. Pour le déchiffrement, les conditions préalables énumérées s'appliquent aussi.

18.1.1.2 Chiffrement basé sur volume et partition du système Windows 7

Pour Windows 7 Professionnel, Entreprise et Édition Intégrale, une partition système est créée sur les ordinateurs d'extrémité sans attribution de lettre de lecteur. Cette partition système ne peut pas être chiffrée par SafeGuard Enterprise.

18.1.1.3 Chiffrement basé sur volume et objets du système de fichiers non identifiés

Les objets du système de fichiers non identifiés sont des volumes qui ne peuvent pas être clairement identifiés comme texte brut ou chiffrés par SafeGuard Enterprise. L'accès au volume est refusé s'il existe une stratégie de chiffrement définie pour un objet du système de fichiers non identifié. Si aucune stratégie de chiffrement n'existe, l'utilisateur peut accéder au volume.

Remarque : si une stratégie de chiffrement, dont le paramètre **Clé à utiliser pour le chiffrement** est défini de sorte à permettre la sélection de clé (par exemple, **Toute clé du jeu de clés utilisateur**), existe pour un volume d'objets du système de fichiers non identifiés, un intervalle de temps s'écoule entre l'affichage de la boîte de dialogue de sélection de la clé et le refus de l'accès. Pendant cet intervalle, le volume reste accessible. Le volume est accessible tant que la boîte de dialogue de sélection de clé n'est pas confirmée. Pour éviter cela, spécifiez une clé présélectionnée pour le chiffrement. Retrouvez plus d'informations sur les paramètres de stratégie correspondants à la section Protection des périphériques à la page 135. Cet intervalle de temps existe également pour les volumes d'objets du système de fichiers non identifiés qui sont connectés à un ordinateur d'extrémité, notamment lorsque l'utilisateur a déjà ouvert des fichiers sur le volume lorsque la stratégie de chiffrement prend effet. Dans ce cas, il n'est pas garanti que l'accès au volume sera refusé car cela risque de provoquer une perte de données.

18.1.1.4 Chiffrement des volumes avec la fonctionnalité Autorun activée

Si vous appliquez une stratégie de chiffrement aux volumes pour lesquels Autorun est activé, voici ce qui peut se produire :

- Le volume n'est pas chiffré.
- Si le volume est un objet système fichier non identifié (Unidentified File System Object), l'accès n'est pas refusé.

18.1.1.5 Accès aux volumes chiffrés BitLocker To Go

Si SafeGuard Enterprise est utilisé avec la prise en charge BitLocker To Go activée et si une stratégie de chiffrement SafeGuard Enterprise existe pour un volume chiffré BitLocker To Go, l'accès au volume est refusé. Si aucune stratégie de chiffrement SafeGuard Enterprise n'existe, l'utilisateur peut accéder au volume.

Retrouvez plus d'informations sur BitLocker To Go à la section BitLocker To Go à la page 161.

18.1.2 Chiffrement intégral du disque basé sur fichier

Le chiffrement basé sur fichier garantit que toutes les données sont chiffrées, à part le support d'initialisation et les informations de répertoire. Avec le chiffrement basé sur fichier, même les supports optiques tels que les CD/DVD peuvent être chiffrés. Par ailleurs, les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard Enterprise n'est pas installé, si les stratégies le permettent. Retrouvez plus d'informations à la section SafeGuard Data Exchange à la page 177.

Remarque : les données chiffrées à l'aide du "chiffrement basé sur fichier" ne peuvent pas être compressées. De même, les données compressées ne peuvent pas être chiffrées en utilisant le chiffrement basé sur fichier.

Remarque : les volumes d'initialisation ne sont jamais chiffrés d'après la méthode basée sur fichier. Ils sont automatiquement exclus du chiffrement basé sur fichier, même si une règle correspondante est définie.

Pour appliquer le chiffrement basé sur fichier aux ordinateurs d'extrémité, créez une stratégie du type **Protection des périphériques** et définissez le **Mode de chiffrement du support** sur **Basé sur fichier**.

18.1.2.1 Comportement par défaut lors de l'enregistrement des fichiers

Étant donné que les applications se comportent différemment lors de l'enregistrement des fichiers, SafeGuard Enterprise propose deux façons de gérer des fichiers chiffrés qui ont été modifiés.

Si un fichier est chiffré avec une clé différente de celle par défaut du volume et si vous modifiez le fichier et l'enregistrez, vous pouvez vous attendre à ce que la clé de chiffrement d'origine soit préservée puisque vous modifiez un fichier et n'en créez pas de nouveau. Mais de nombreuses applications enregistrent des fichiers en effectuant une combinaison d'opérations d'enregistrement, de suppression et de changement de nom (par exemple, Microsoft Office). Si elles font ça, le paramètre SafeGuard Enterprise par défaut est d'utiliser la clé par défaut pour cette tâche de chiffrement et donc de changer la clé utilisée pour le chiffrement.

Si vous voulez changer ce comportement et préserver la clé utilisée pour le chiffrement dans tous les cas, vous pouvez modifier une clé de registre sur l'ordinateur d'extrémité.

Pour toujours utiliser la même clé lors de l'enregistrement des fichiers modifiés :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UTIMACO\SGLCENC]
"ActivateEncryptionTunneling"=dword:00000001
```

Pour permettre l'utilisation d'une clé différente (clé par défaut) lors de l'enregistrement des fichiers modifiés. Il s'agit du paramètre par défaut après l'installation :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UTIMACO\SGLCENC]
"ActivateEncryptionTunneling"=dword:00000000
```

Remarque : les changements de ce paramètre seront appliqués suite au redémarrage de l'ordinateur d'extrémité.

18.2 Chiffrement de lecteur BitLocker

Le Chiffrement de lecteur BitLocker est une fonction de chiffrement de disque complet avec authentification de préinitialisation incluse dans les systèmes d'exploitation Microsoft Windows. Elle est conçue pour protéger les données en permettant le chiffrement des volumes d'initialisation et de données.

SafeGuard Enterprise gère le chiffrement BitLocker sur un ordinateur. Le chiffrement BitLocker peut être activé et la gestion des lecteurs déjà chiffrés par BitLocker peut être prise en charge.

Pendant l'installation sur l'ordinateur d'extrémité et pendant le premier redémarrage, SafeGuard Enterprise détermine si le matériel satisfait aux conditions requises pour BitLocker avec le Challenge/Réponse SafeGuard. S'il ne satisfait pas aux conditions, la gestion de SafeGuard Enterprise BitLocker s'effectue sans Challenge/Réponse. Dans ce cas, la clé de récupération BitLocker peut être récupérée à l'aide de SafeGuard Management Center.

Remarque : pour Windows 8 et Windows 8.1, seul le Chiffrement de lecteur BitLocker peut être utilisé pour le chiffrement intégral du disque.

18.2.1 Authentification avec le Chiffrement de lecteur BitLocker

Le Chiffrement de lecteur BitLocker propose un large éventail d'options d'authentification. Les utilisateurs BitLocker peuvent s'authentifier avec un TPM (module de plate-forme sécurisée) ou une carte mémoire USB ou une combinaison des deux.

Le responsable de la sécurité peut définir les différents modes de connexion dans une stratégie dans SafeGuard Management Center et la distribuer aux ordinateurs d'extrémité BitLocker.

Les modes de connexion suivants sont proposés aux utilisateurs SafeGuard Enterprise BitLocker :

- TPM

- TPM + PIN
- TPM + carte mémoire USB
- Carte mémoire USB (sans TPM)

Remarque : si vous voulez utiliser l'un des modes de connexion **TPM + PIN**, **TPM + Carte mémoire USB** ou **Carte mémoire USB**, veuillez activer la Stratégie de groupe **Authentification supplémentaire requise au démarrage** soit dans Active Directory, soit localement sur les ordinateurs.

La Stratégie de groupe est automatiquement activée lors de l'installation sur l'ordinateur d'extrémité. Assurez-vous que les paramètres ne sont pas remplacés par différents Stratégies de groupe.

Pour vérifier les paramètres, ouvrez l'Éditeur d'objets de stratégie de groupe : **Démarrer - Exécuter - gpedit.msc** et sélectionnez **Stratégie de l'ordinateur local - Configuration ordinateur - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker - Lecteur du système d'exploitation** et cliquez deux fois sur **Demander une authentification supplémentaire au démarrage**. La case **Activer** doit être sélectionnée.

Pour le mode de connexion **Carte mémoire USB**, la case **Autoriser BitLocker sans un module de plateforme sécurisée compatible (requiert une clé de démarrage sur un lecteur flash USB)** doit également être sélectionnée.

18.2.1.1 TPM (module de plate-forme sécurisée)

TPM est un module semblable à une carte à puce sur la carte mère qui exécute des fonctions cryptographiques et des opérations de signature numérique. Il permet de créer, stocker et gérer des clés utilisateur. Il est protégé contre les attaques.

18.2.1.2 Clé USB

Les clés externes peuvent être stockées sur une clé USB non protégée.

18.2.2 Conditions préalables à la gestion de BitLocker sur les ordinateurs d'extrémité

- Si vous voulez utiliser l'une des méthodes de connexion **TPM + PIN**, **TPM + Carte mémoire USB** ou **Carte mémoire USB**, veuillez activer la Stratégie de groupe **Authentification supplémentaire requise au démarrage** soit dans Active Directory, soit localement sur les ordinateurs. Dans l'Éditeur d'objets de stratégie de groupe (gpedit.msc), la Stratégie de groupe se trouve à l'emplacement suivant : Stratégie de l'ordinateur local\Configuration ordinateur\Modèles d'administration\Composants Windows\Chiffrement de lecteur BitLocker\Lecteur du système d'exploitation.

  Pour utiliser la méthode **Carte mémoire USB**, veuillez également activer **Autoriser BitLocker sans un module de plateforme sécurisée compatible** dans la Stratégie de groupe.

- Pour utiliser la méthode **TPM + PIN** sur les tablettes, veuillez également activer la Stratégie de groupe **Activer l'utilisation de l'authentification BitLocker exigeant une saisie au clavier préalable au démarrage sur tablettes tactiles**.

Remarque : ces Stratégies de groupe sont automatiquement activées lors de l'installation sur l'ordinateur d'extrémité. Assurez-vous que les paramètres ne sont pas remplacés par différents Stratégies de groupe.

- Le module de plate- forme sécurisée ou TPM de l'ordinateur doit être activé et la propriété doit être définie avant que SafeGuard Enterprise ne puisse gérer le chiffrement BitLocker.

  Remarque : si la gestion de SafeGuard BitLocker est installée sur un ordinateur d'extrémité, il se peut que l'état de chiffrement d'un lecteur indique **Non préparé**. Ceci signifie que le lecteur ne peut actuellement pas être chiffré avec BitLocker car les préparations d'usage n'ont pas encore été effectuées. Ceci s'applique uniquement aux ordinateurs d'extrémité administrés. En effet, les ordinateurs d'extrémité non administrés ne sont pas en mesure de créer des rapports sur les données d'inventaire.

  Retrouvez plus d'informations à la section Onglet Lecteurs à la page 250.

  L'état du système d'un ordinateur d'extrémité non administré peut être vérifié à l'aide de l'outil de ligne de commande SGNState. Retrouvez plus d'informations dans le *Guide des outils de SafeGuard Enterprise*.

Challenge/Réponse SafeGuard pour BitLocker

L'utilisation du Challenge/Réponse SafeGuard Enterprise pour BitLocker nécessite de satisfaire aux conditions ci-dessous :

- Windows 64-bits
- Version UEFI 2.3.1 ou plus récente
- Certificat UEFI de Microsoft activé ou Démarrage sécurisé désactivé
- Entrées de démarrage NVRAM accessibles à partir de Windows
- Windows installé en mode GPT
- Le matériel ne doit pas être répertorié dans le fichier POACFG.xml.

  Sophos fournit un fichier POACFG.xml par défaut intégré dans le programme d'installation. Nous vous conseillons de télécharger le fichier le plus récent et de le mettre à disposition du programme d'installation.

Pendant l'installation sur l'ordinateur d'extrémité et pendant le premier redémarrage, SafeGuard Enterprise détermine si le matériel satisfait aux conditions requises pour BitLocker avec le Challenge/Réponse SafeGuard. S'il ne satisfait pas aux conditions, la gestion de SafeGuard Enterprise BitLocker s'effectue sans Challenge/Réponse. Dans ce cas, la clé de récupération BitLocker peut être récupérée à l'aide de SafeGuard Policy Editor.

18.2.3 Gestion du Chiffrement de lecteur BitLocker avec SafeGuard Enterprise

SafeGuard Enterprise vous permet de gérer le Chiffrement de lecteur BitLocker à partir de SafeGuard Management Center pareillement à un client SafeGuard Enterprise natif. En tant que responsable de la sécurité, vous pouvez définir des stratégies de chiffrement et d'authentification pour les ordinateurs d'extrémité BitLocker et les distribuer.

Lors de l'installation du client SafeGuard Enterprise, la fonction **BitLocker** doit être explicitement sélectionnée pour activer la gestion de BitLocker.

Lorsque l'ordinateur d'extrémité BitLocker est enregistré dans SafeGuard Enterprise, les informations concernant l'utilisateur, l'ordinateur, le mode de connexion et l'état du chiffrement apparaissent. Les événements sont également consignés dans le journal pour les clients BitLocker.

La gestion des clients BitLocker dans SafeGuard Enterprise est transparente, ce qui signifie que les fonctions de gestion fonctionnent en général de façon identique pour les clients BitLocker et SafeGuard Enterprise natifs. Vous pouvez retrouver plus d'informations sur le type d'un ordinateur dans l'**Inventaire** d'un conteneur dans **Utilisateurs et ordinateurs**. La colonne **Type de chiffrement** vous indique si l'ordinateur correspondant est un client BitLocker.

La gestion centralisée et totalement transparente de BitLocker via SafeGuard Enterprise permet ainsi de l'utiliser dans des environnements informatiques hétérogènes. SafeGuard Enterprise améliore de manière considérable les fonctions BitLocker. Les stratégies de sécurité de BitLocker peuvent être appliquées de manière centralisée via SafeGuard Enterprise. Même des processus critiques, comme la gestion et la récupération des clés, sont disponibles lorsque BitLocker est géré par l'intermédiaire de SafeGuard Enterprise.

Retrouvez plus d'informations sur la prise en charge SafeGuard Enterprise de l'amélioration BitLocker To Go dans Windows 7 et Windows 8 à la section BitLocker To Go à la page 161.

18.2.4 Chiffrement avec BitLocker à l'aide de SafeGuard Enterprise

Avec la prise en charge de BitLocker Drive Encryption dans SafeGuard Enterprise, vous pouvez chiffrer les éléments suivants :

- Volume d'initialisation avec le chiffrement BitLocker et les clés BitLocker
- Autres volumes avec le chiffrement BitLocker et les clés BitLocker
- Toutes les données, par exemple, de support amovible avec le chiffrement de fichiers de SafeGuard Enterprise et les clés SafeGuard Enterprise.

18.2.4.1 Clés de chiffrement pour BitLocker

Lors d'un chiffrement du volume d'initialisation ou d'autres volumes avec BitLocker via SafeGuard Enterprise, les clés de chiffrement sont toujours générées par BitLocker. Une clé est générée par BitLocker pour chaque volume et ne peut pas être réutilisée. Elle doit être stockée en lieu sûr.

Lors de l'utilisation de BitLocker avec SafeGuard Enterprise, une clé de sauvegarde est stockée dans la base de données SafeGuard Enterprise de clés générées par BitLocker. Ceci permet de définir un mécanisme d'assistance et de récupération similaire au mécanisme de Challenge/Réponse de SafeGuard Enterprise.

Il n'est cependant pas possible de sélectionner globalement des clés et de les réutiliser avec des clients SafeGuard Enterprise natifs. Les clés n'apparaissent pas dans le SafeGuard Management Center.

Remarque : si un volume est chiffré alors que la prise en charge SafeGuard Enterprise BitLocker est déjà installée, l'administrateur peut enregistrer les clés de sauvegarde (protégées par un

mot de passe de récupération) dans Active Directory, en plus du stockage dans la base de données SafeGuard Enterprise. L'administrateur doit le faire manuellement à l'aide de l'outil Windows Manage BDE et en les enregistrant dans une stratégie de groupe. En revanche, pour Windows 2003 Server, le schéma Active Directory utilisé doit être étendu. En outre, des droits d'administrateur de domaine sont nécessaires pour récupérer les informations stockées.

18.2.4.2 Algorithmes BitLocker dans SafeGuard Enterprise

BitLocker prend en charge les algorithmes AES (Advanced Encryption Standard) suivants:

- AES-128
- AES-256
- AES-128 avec diffuseur
- AES-256 avec diffuseur

Le diffuseur est spécifique à BitLocker et ne peut pas être utilisé en mode de chiffrement de volumes de SafeGuard Enterprise. Microsoft déconseille l'utilisation de cet algorithme avec ce diffuseur. Les lecteurs déjà chiffrés utilisant un algorithme avec un diffuseur peuvent être gérés par Sophos SafeGuard. Pour les lecteurs devant être chiffrés, il n'est pas possible de sélectionner les algorithmes avec diffuseur.

AES-128 avec diffuseur et AES-256 avec diffuseur ne sont pas disponibles dans Windows 8.

18.2.4.3 Stratégies de chiffrement pour le Chiffrement de lecteur BitLocker

Le responsable de la sécurité peut créer une stratégie de chiffrement (initial) dans le SafeGuard Management Center et la distribuer aux ordinateurs d'extrémité BitLocker lors de l'exécution. Elle déclenche le chiffrement BitLocker des lecteurs indiqués dans la stratégie.

Les clients BitLocker étant administrés de manière transparente dans le SafeGuard Management Center, le responsable de la sécurité ne doit procéder à aucun paramétrage BitLocker spécifique pour le chiffrement. SafeGuard Enterprise connait le statut du client et sélectionne en conséquence le chiffrement BitLocker. Lorsqu'un client BitLocker est installé avec SafeGuard Enterprise et que le chiffrement de volumes est activé, les volumes sont chiffrés par BitLocker Drive Encryption.

Un ordinateur d'extrémité Bitlocker traite les stratégies de type **Protection des périphériques** et **Authentification**.

Les paramètres suivants sont évalués sur l'ordinateur d'extrémité :

- Paramètres d'une stratégie de type **Protection des périphériques** :
  - **Cible :**
  - **Mode de chiffrement des supports :Basé sur le volume | Aucun chiffrement**
  - **Algorithme à utiliser pour le chiffrement :AES128 | AES256**
  - **Chiffrement initial rapide :Oui | Non**

Retrouvez plus d'informations à la section Protection des périphériques à la page 135.

- Sélectionnez une stratégie du type **Authentification**.
  - **Mode de connexion BitLocker :TPM | TPM + PIN | TPM + carte mémoire USB | Carte mémoire USB |**
  - **Mode de connexion de secours BitLocker : Erreur**

Retrouvez plus d'informations à la section Authentification à la page 117.

Tous les autres paramètres sont ignorés par l'ordinateur d'extrémité BitLocker.

18.2.4.4 Chiffrement sur un ordinateur protégé par BitLocker

Avant toute opération de chiffrement, les clés de chiffrement et de déchiffrement sont générées par BitLocker. Le comportement est légèrement différent selon le système utilisé et la prise en charge de la version de SafeGuard BitLocker qui est installée.

Ordinateurs d'extrémité avec TPM

BitLocker conserve ses propres clés de chiffrement et de déchiffrement dans un matériel de sécurité nommé Module de plate-forme sécurisée (TPM ou Trusted Platform Module). Les clés ne sont pas stockées sur le disque dur de l'ordinateur. Le module TPM doit être accessible par le BIOS au cours du démarrage. Lorsque vous démarrez votre ordinateur, BitLocker récupère ces clés automatiquement à partir du TPM.

Votre responsable de la sécurité peut définir différents mode de connexion (TPM, TPM+PIN ou TPM + carte mémoire USB) pour BitLocker. Lorsque SafeGuard Enterprise active BitLocker, la clé de démarrage de BitLocker est stockée sur le TPM.

Remarque : le TPM doit être activé et la propriété doit être définie avant que SafeGuard Enterprise ne puisse gérer le chiffrement BitLocker.

Ordinateurs d'extrémité sans TPM

Si un ordinateur n'est pas équipé d'un module de plate-forme sécurisée (TPM), vous pouvez créer une clé de démarrage BitLocker à l'aide d'un lecteur flash USB pour stocker les clés de chiffrement et de déchiffrement. Veuillez insérer le lecteur flash à chaque fois que vous allumez l'ordinateur.

Lorsque SafeGuard Enterprise active BitLocker, vous êtes invité à procéder à l'enregistrement de la clé de démarrage BitLocker. Une boîte de dialogue affiche les lecteurs cibles dans lesquels vous pouvez stocker la clé de démarrage.

Remarque : pour les **volumes d'initialisation,** il est essentiel que vous disposiez de la clé de démarrage lorsque vous allumez votre ordinateur. Par conséquent, le stockage de la clé de démarrage est limité aux supports amovibles.

Pour les volumes de données, vous pouvez stocker la clé de démarrage BitLocker sur un volume d'initialisation déjà chiffré. Si le volume est chiffré, il apparaît sous **Lecteurs cibles corrects** et peut être sélectionné.

Clés de récupération BitLocker

Pour la récupération BitLocker, SafeGuard Enterprise propose une procédure Challenge/Réponse pour l'échange d'informations confidentielles ainsi que la possibilité

d'obtenir la clé de récupération à partir du support. Retrouvez plus d'informations aux sections Réponse pour les clients SafeGuard Enterprise chiffrés par BitLocker : ordinateurs d'extrémité UEFI à la page 229 et Clé de récupération pour les clients SafeGuard Enterprise chiffrés par BitLocker : ordinateurs d'extrémité BIOS à la page 229.

Pour permettre la récupération par Challenge/Réponse ou l'obtention de la clé de récupération, le support technique doit avoir les données nécessaires à disposition. Ces données nécessaires à la récupération sont enregistrées dans des fichiers de récupération de clé spécifiques.

Remarque : si la gestion de SafeGuard BitLocker sans Challenge/Réponse en mode autonome est utilisée, la clé de récupération ne change pas suite à la procédure de récupération.

Remarque : si un disque dur chiffré BitLocker sur un ordinateur est remplacé par un nouveau disque dur chiffré BitLocker et que celui-ci prend la même lettre de lecteur que le précédent, SafeGuard Enterprise n'enregistre que la clé de récupération du nouveau disque.

Gestion des lecteurs déjà chiffrés avec BitLocker

Lorsque vous disposez de lecteurs déjà chiffrés avec BitLocker sur votre ordinateur, ils seront gérés par SafeGuard Enterprise dès que le logiciel sera installé.

Lecteurs d'initialisation chiffrés

- Selon la prise en charge SafeGuard Enterprise BitLocker utilisée, il se peut que vous deviez redémarrer l'ordinateur. Veuillez redémarrer l'ordinateur aussitôt que possible.
- Une stratégie de chiffrement SafeGuard Enterprise s'applique au lecteur chiffré :
  - Le **Challenge/Réponse SafeGuard Enterprise BitLocker** est installé : la gestion est prise en charge et il est possible d'utiliser le Challenge/Réponse SafeGuard Enterprise.
  - **SafeGuard Enterprise BitLocker** est installé : la gestion est prise en charge et il est possible d'utiliser la récupération.
- Aucune stratégie de chiffrement SafeGuard Enterprise ne s'applique au lecteur chiffré :
  - Le **Challenge/Réponse SafeGuard Enterprise BitLocker** est installé : la gestion n'est pas prise en charge et il n'est pas possible d'utiliser le Challenge/Réponse SafeGuard Enterprise.
  - **SafeGuard Enterprise BitLocker** est installé : il est possible d'utiliser la récupération.

Lecteurs de données chiffrés

- Une stratégie de chiffrement SafeGuard Enterprise s'applique au lecteur chiffré :

  la gestion est prise en charge et il est possible d'utiliser la récupération.
- Aucune stratégie de chiffrement SafeGuard Enterprise ne s'applique au lecteur chiffré :

  il est possible d'utiliser la récupération SafeGuard Enterprise.

18.2.4.5 Déchiffrement avec BitLocker

Les ordinateurs chiffrés avec BitLocker ne peuvent pas être déchiffrés automatiquement. Le déchiffrement doit être exécuté à l'aide de l'outil « Manage-bde » de Microsoft. Cet outil de

ligne de commande peut être utilisé à la place de l'élément **Chiffrement de lecteur BitLocker** du **Panneau de configuration**.

Pour permettre aux utilisateurs de déchiffrer les lecteurs chiffrés avec BitLocker manuellement, une stratégie sans règle de chiffrement pour le lecteur chiffré par BitLocker doit être appliquée sur l'ordinateur d'extrémité. L'utilisateur peut déclencher le chiffrement en désactivant BitLocker pour le lecteur de son choix à partir de l'élément **Chiffrement de lecteur BitLocker** du **Panneau de configuration**.

18.2.5 BitLocker To Go

Avec BitLocker To Go, la fonctionnalité de Chiffrement de lecteur BitLocker a été étendue dans Microsoft Windows 7. Elle permet aux utilisateurs de chiffrer des volumes internes ainsi que des volumes sur supports amovibles connectés aux ordinateurs d'extrémité à partir du menu contextuel de l'Explorateur Windows.

- Lorsque le client de chiffrement des périphériques de SafeGuard Enterprise a été déployé avec la "prise en charge BitLocker" activée, BitLocker To Go est pris en charge.
- Lorsque le client de chiffrement des périphériques de SafeGuard Enterprise a été déployé sans activer la "prise en charge BitLocker" ou lorsque le client SafeGuard Data Exchange a été déployé, le chiffrement avec BitLocker To Go n'est pas compatible et doit être dans ce cas désactivé. Par contre, le chiffrement des volumes internes et des supports amovibles peut être correctement configuré de manière centralisée dans les stratégies de sécurité SafeGuard Enterprise. Les volumes et les supports amovibles qui ont été chiffrés avec BitLocker To Go avant le déploiement de SafeGuard Enterprise restent lisibles.

18.2.5.1 Désactivation du chiffrement BitLocker To Go

1. Dans l'éditeur de stratégies de groupes Windows, sélectionnez **Stratégie de domaine par défaut** > **Configuration ordinateur** > **Stratégies** > **Modèles d'administration (ordinateur local)**> **Composants Windows** > **Chiffrement de lecteur BitLocker** > **Lecteurs de données amovibles**.
2. Sous **Lecteurs de données amovibles**, sélectionnez la stratégie suivante : **Contrôler l'utilisation de BitLocker sur les lecteurs amovibles**. Définissez les options comme suit :
   a) Sélectionnez **Activé**.
   b) Sous **Options**, dessélectionnez **Autoriser les utilisateurs à protéger les lecteurs de données amovibles avec BitLocker**.
   c) Sous **Options**, sélectionnez **Autoriser les utilisateurs à suspendre et supprimer la protection BitLocker sur les lecteurs de données amovibles**.
3. Cliquez sur **OK**.

Le chiffrement BitLocker To Go est désactivé sur les ordinateurs d'extrémité. Les utilisateurs ne peuvent plus chiffrer les nouveaux volumes avec BitLocker To Go. Les volumes chiffrés avec BitLocker To Go avant le déploiement du client de chiffrement des périphériques de SafeGuard Enterprise natif restent lisibles.

Les paramètres du registre obtenus côté client sont comme suit :

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE]

"RDVConfigureBDE"=dword:00000001

"RDVAllowBDE"=dword:00000000

"RDVDisableBDE"=dword:00000001

Ces clés de registre sont aussi paramétrées lors de l'installation du client de chiffrement des périphériques de SafeGuard Enterprise afin que BitLocker To Go soit aussi désactivé sur les ordinateurs sans administration de domaine comme les ordinateurs de groupe de travail ou autonomes.

18.2.6 Journalisation

Les événements signalés par le client BitLocker sont consignés dans le journal de la même manière que pour tout autre client SafeGuard Enterprise. Il n'est pas expressément indiqué que l'événement est lié à un client BitLocker. Les événements signalés sont identiques pour tout client SafeGuard Enterprise.

18.3 Chiffrement intégral du disque FileVault 2

FileVault 2 est une technologie de chiffrement intégrée à OS X qui protège un volume tout entier et qui peut être gérée par SafeGuard Enterprise.

18.3.1 Gestion du chiffrement intégral du disque FileVault 2 avec SafeGuard Enterprise

SafeGuard Enterprise vous permet de gérer le chiffrement intégral du disque FileVault 2 à partir de SafeGuard Management Center pareillement à un client SafeGuard Enterprise natif.

L'installation du client SafeGuard Enterprise ne contient pas le composant de gestion de FileVault 2. Il doit être installé séparément. Retrouvez plus de renseignements dans votre documentation de Sophos SafeGuard Disk Encryption pour Mac.

La gestion centralisée et totalement transparente de FileVault 2 par SafeGuard Enterprise permet ainsi de l'utiliser dans des environnements informatiques hétérogènes. Les stratégies de sécurité de différentes plates-formes peuvent être déployées de manière centralisée.

18.3.2 Gestion des ordinateurs d'extrémité FileVault 2 avec SafeGuard Management Center

Dans SafeGuard Management Center, les ordinateurs d'extrémité FileVault 2 peuvent être gérés exactement comme tout ordinateur d'extrémité natif de SafeGuard Enterprise. En tant que responsable de la sécurité, vous pouvez définir des stratégies de chiffrement pour les ordinateurs d'extrémité FileVault 2 et les distribuer.

Lorsque l'ordinateur d'extrémité FileVault 2 est enregistré dans SafeGuard Enterprise, les informations concernant l'utilisateur, l'ordinateur, le mode de connexion et l'état du chiffrement apparaissent. Les événements sont également consignés dans le journal pour les clients FileVault 2.

La gestion des clients FileVault 2 dans SafeGuard Enterprise est transparente, ce qui signifie que les fonctions de gestion fonctionnent en général de façon identique pour les clients FileVault 2 et SafeGuard Enterprise natifs. Vous pouvez retrouver plus d'informations sur le type d'un ordinateur dans l'**Inventaire** d'un conteneur dans **Utilisateurs et ordinateurs**. La colonne **Type de chiffrement** vous indique si l'ordinateur correspondant est un client FileVault2.

18.3.3 Stratégies de chiffrement pour le chiffrement intégral du disque FileVault 2

Le responsable de la sécurité peut créer une stratégie de chiffrement dans SafeGuard Management Center et la distribuer aux ordinateurs d'extrémité FileVault 2 sur lesquels elle sera appliquée.

Les ordinateurs d'extrémité FileVault 2 étant administrés de manière transparente dans SafeGuard Management Center, le responsable de la sécurité n'a pas besoin de procéder à un paramétrage spécifique de FileVault 2 pour le chiffrement. SafeGuard Enterprise connait l'état du client et sélectionne en conséquence le chiffrement FileVault 2.

Un ordinateur d'extrémité FileVault 2 traite uniquement les stratégies de type **Protection des périphériques** avec des **Volumes d'initialisation** cibles et le **Mode de chiffrement du support** défini sur **Volume** ou sur **Aucun chiffrement**. Tous les autres paramètres de stratégie sont ignorés.

- **Volume** active FileVault 2 sur l'ordinateur d'extrémité.
- **Aucun chiffrement** permet à l'utilisateur de déchiffrer le Mac.

19 Protection de la configuration SafeGuard

Le module Protection de la configuration de SafeGuard n'est plus disponible dans SafeGuard Enterprise 6.1. La stratégie correspondante est toujours disponible dans la version 6.1 de SafeGuard Management Center afin de prendre en charge les clients SafeGuard Enterprise 6 qui ont installé la Protection de la configuration et qui veulent l'administrer avec la version 6.1 du Management Center.

Retrouvez plus d'informations sur la Protection de la configuration de SafeGuard dans l'Aide de l'administrateur de SafeGuard Enterprise 6.
http://www.sophos.com/fr-fr/medialibrary/PDFs/documentation/sgn_60_h_eng_admin_help.pdf.

20 Utilisation de File Encryption avec File Share

Le module File Share de SafeGuard Enterprise offre un chiffrement de fichiers sur les lecteurs locaux et les emplacements réseau, surtout pour les groupes de travail et les partages réseau.

Dans SafeGuard Management Center, vous définissez les règles du chiffrement basé sur fichier dans les stratégies **File Encryption**. Dans ces règles File Encryption, vous indiquez les dossiers qui doivent être gérés par File Encryption, le mode de chiffrement et la clé à utiliser pour le chiffrement. Dans les stratégies **Paramètres généraux**, vous pouvez définir comment des applications et des systèmes de fichiers spécifiques sont gérés sur les ordinateurs d'extrémité dans le contexte de File Encryption. Vous pouvez indiquer les applications ignorées et fiables ainsi que les périphériques ignorés. Vous pouvez aussi activer le chiffrement permanent pour File Encryption.

Pour le chiffrement, des clés personnelles peuvent être utilisées. Une clé personnelle activée pour un utilisateur particulier s'applique uniquement à cet utilisateur et ne peut pas être partagée avec d'autres utilisateurs ou attribuée à ces derniers. Vous pouvez créer des clés personnelles dans le SafeGuard Management Center sous **Utilisateurs et ordinateurs**.

Après attribution d'une stratégie **File Encryption** sur vos ordinateurs d'extrémité, les fichiers présents dans les emplacements couverts par la stratégie sont chiffrés de manière transparente sans intervention de l'utilisateur :

- Les nouveaux fichiers dans les emplacements correspondants sont chiffrés automatiquement.
- Si les utilisateurs ont la clé d'un fichier chiffré, ils peuvent lire et modifier le contenu.
- S'ils n'ont pas la clé du fichier chiffré, l'accès est refusé.
- Si un utilisateur accède à un fichier chiffré sur un ordinateur d'extrémité sur lequel File Encryption n'est pas installé, le contenu chiffré apparaît.

Les fichiers déjà présents dans les emplacements couverts par la stratégie de chiffrement ne sont pas chiffrés automatiquement. Les utilisateurs doivent procéder au chiffrement initial dans l' **Assistant de chiffrement de fichiers SafeGuard** sur l'ordinateur d'extrémité. Retrouvez plus d'informations dans le *Manuel d'utilisation de SafeGuard Enterprise*.

Remarque :

SafeGuard File Share n'est pas compatible avec le chiffrement EFS intégré et la compression de fichiers de Windows. Si EFS est activé, il est prioritaire sur toute règle de chiffrement de fichiers applicable et les fichiers créés dans le dossier en question ne peuvent pas être chiffrés par File Encryption. Si la compression est activée, File Encryption a une priorité plus haute et les fichiers sont chiffrés mais pas compressés. Pour chiffrer les fichiers avec File Encryption, veuillez d'abord supprimer le chiffrement EFS ou la compression des données. L'opération peut être effectuée manuellement ou en exécutant l'assistant de chiffrement initial de SafeGuard Enterprise.

Remarque :

Retrouvez plus de renseignements sur l'utilisation d'ordinateurs d'extrémité Mac et de SafeGuard File Encryption pour Mac dans les documents ci-dessous :

- *Guide de démarrage rapide de SafeGuard File Encryption pour Mac.*

Ce document s'adresse aux utilisateurs d'ordinateurs Mac.

- *Manuel d'administration de SafeGuard File Encryption pour Mac.*

  Ce document s'adresse aux administrateurs travaillant conjointement sur les plates-formes Mac et Windows.

20.1 Configuration des règles de chiffrement dans les stratégies File Encryption

Vous définissez les règles du chiffrement basé sur fichier sur les emplacements réseau dans une stratégie du type **File Encryption** .

Remarque : lorsqu'ils sont chiffrés, certains dossiers (par exemple, c:\program files) peut empêcher l'exécution du système d'exploitation ou d'applications. Lorsque vous définissez des règles de chiffrement, assurez-vous que ces dossiers ne sont pas chiffrés.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **File Encryption** ou sélectionnez-en une.

   Le tableau des règles de la stratégie **File Encryption** apparaît.

2. Dans la colonne **Chemin**, définissez le chemin (c'est-à-dire le dossier) à gérer par File Encryption :

   - Cliquez sur le bouton déroulant et sélectionnez un espace réservé de nom de dossier dans la liste des espaces réservés disponibles.

     Remarque : en faisant passer votre curseur sur les entrées de la liste, vous pouvez afficher des infobulles qui vous indiquent comment un espace réservé est généralement présenté sur un ordinateur d'extrémité. Vous pouvez seulement saisir des espaces réservés valides. Retrouvez une description de tous les espaces réservés disponibles à la section Espaces réservés pour les chemins des règles File Encryption à la page 169.

     Remarque : le chiffrement intégral du profil utilisateur à l'aide de l'espace réservé <Profil utilisateur> peut entraîner une instabilité du bureau Windows sur l'ordinateur d'extrémité.

   - Cliquez sur le bouton Parcourir pour naviguer dans le système de fichiers et sélectionnez le dossier requis.
   - Sinon, entrez simplement un nom de chemin.

   Remarque : retrouvez plus d'informations sur les chemins de configuration dans les règles File Encryption à la section Informations supplémentaires sur la configuration des chemins dans les règles File Encryption à la page 168.

3. Dans la colonne **Étendue**, sélectionnez

   - **Seulement ce dossier** pour appliquer la règle seulement au dossier indiqué par la colonne **Chemin**, ou
   - **Inclure les sous-dossiers** pour appliquer aussi la règle à tous ses sous-dossiers.

4. Dans la colonne **Mode**, définissez comment File Encryption doit gérer le dossier indiqué dans la colonne **Chemin** :

   - Sélectionnez **Chiffrer** pour chiffrer de nouveaux fichiers dans le dossier. Le contenu des fichiers chiffrés existants est déchiffré de manière transparente lorsqu'un utilisateur y accède avec la clé requise. Si l'utilisateur n'a pas la clé requise, l'accès est refusé.
   - Si vous sélectionnez **Exclure**, les nouveaux fichiers du dossier ne sont pas chiffrés. Vous pouvez utiliser cette option pour exclure un sous-dossier du chiffrement si le dossier parent est déjà couvert par une règle avec l'option **Chiffrer**.
   - Si vous sélectionnez **Ignorer**, les fichiers du dossier ne sont pas gérés du tout par File Encryption. Les nouveaux fichiers sont enregistrés en texte simple. Si un utilisateur accède déjà aux fichiers chiffrés dans ce dossier, le contenu chiffré apparaît, que l'utilisateur ait la clé requise ou pas.

5. Dans la colonne **Clé**, sélectionnez la clé à utiliser pour le mode **Chiffrer**. Vous pouvez utiliser des clés créées et appliquées dans **Utilisateurs et ordinateurs** :

   - Cliquez sur le bouton Parcourir pour ouvrir la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour afficher une liste de toutes les clés disponibles et sélectionnez la clé requise.

     Remarque : les clés machine ne sont pas montrées dans la liste. Elles ne peuvent pas être utilisées par File Encryption car elles sont uniquement disponibles sur une seule machine et ne peuvent donc pas être utilisées pour permettre à des groupes d'utilisateurs d'accéder aux mêmes données.

   - Clique sur le bouton **Clé personnelle** avec l'icône de la clé, pour insérer l'espace réservé **Clé personnelle** dans la colonne **Clé**. Sur l'ordinateur d'extrémité, cet espace réservé sera résolu sur la clé personnelle active de l'utilisateur SafeGuard Enterprise connecté. Si les utilisateurs correspondants n'ont pas encore de clés personnelles actives, elles sont créées automatiquement. Vous pouvez créer des clés personnelles pour un ou plusieurs utilisateurs dans **Utilisateurs et ordinateurs**. Retrouvez plus d'informations à la section Clés personnelles pour le chiffrement de fichiers par File Share à la page 57.

6. Le type de **Système** (**Windows**, **Mac OS X** ou **Tous les systèmes** pour les systèmes Windows et Mac OSX) sera attribué automatiquement.
7. Ajoutez d'autres règles de chiffrement selon vos besoins et enregistrez vos changements.

   Remarque : toutes les règles File Encryption attribuées par des stratégies et activées pour les utilisateurs/ordinateurs à des nœuds différents dans **Utilisateurs et ordinateurs** sont cumulées. L'ordre des règles de chiffrement dans une stratégie **File Encryption** n'a pas d'importance pour leur évaluation sur l'ordinateur d'extrémité. Dans une stratégie **File Encryption**, vous pouvez déplacer les règles pour avoir une meilleur visibilité.

20.1.1 Informations supplémentaires sur la configuration des chemins dans les règles File Encryption

Lors de la configuration des chemins dans les règles File Encryption, veuillez prendre en compte ce qui suit.

- Un chemin peut seulement contenir des caractères qui peuvent aussi être utilisés dans des systèmes de fichiers. Les caractères comme <, >, * et $ ne sont pas autorisés.
- Vous pouvez seulement saisir des espaces réservés valides. Retrouvez une liste des espaces réservés autorisés à la section Espaces réservés pour les chemins des règles File Encryption à la page 169.

  Remarque : les noms des variables d'environnement ne sont pas vérifiés par SafeGuard Management Center. Ils doivent seulement être présents sur l'ordinateur d'extrémité.

- Le champ **Chemin** indique toujours un dossier. Vous ne pouvez pas spécifier de fichier unique ou utiliser de caractères joker pour les noms de dossiers, de fichiers ou pour les extensions de fichiers.
- **Règles absolues et relatives**

  Vous pouvez définir des règles absolues et relatives. Une règle absolue définit exactement un dossier spécifique, par exemple **`C:\encrypt`**. Une règle relative n'inclut pas d'informations sur le serveur/partage UNC, d'informations sur la lettre du lecteur ou sur le dossier parent. **`encrypt_sub`** est un exemple de chemin utilisé dans une règle relative. Dans ce cas, tous les fichiers présents sur tous les lecteurs (y compris les emplacements réseau) qui résident dans un dossier **`encrypt_sub`** (ou l'un de ses sous-dossiers) sont couverts par la règle.

- **Noms de dossiers longs et notation 8.3**

  Saisissez toujours les noms de dossiers longs pour les règles File Encryption car les noms 8.3 pour les noms de dossiers longs peuvent varier d'un ordinateur à un autre. Les règles des noms 8.3 sont détectées automatiquement par l'ordinateur d'extrémité protégé par SafeGuard Enterprise lorsque les stratégies correspondantes sont appliquées. Que les applications utilisent des noms de dossiers longs ou des noms 8.3 pour l'accès aux fichiers, le résultat devrait être identique. Pour les règles relatives, utilisez des noms de dossiers courts pour vous assurer que la règle peut être appliquée, que l'application utilise ou non des noms de dossiers longs ou une notation 8.3.

- **Notation UNC et/ou lettres des lecteurs mappés**

  Que l'administration des règles soit basée sur une notation UNC ou sur des lettres de lecteurs mappés dépend de vos conditions requises :

  - Utilisez la notation UNC si vos noms de serveur et de partage ne sont pas susceptibles de changer, mais si les mappages des lettres de lecteurs varient entre les utilisateurs.
  - Utilisez des lettres de lecteurs mappés, si les lettres restent les mêmes et si les noms des serveurs peuvent changer.

  Si vous utilisez UNC, spécifiez un nom de serveur et un nom de partage, par exemple \\serveur\partage.

File Encryption fait correspondre en interne les noms UNC et les lettres de lecteurs mappés. Dans une règle, un chemin a donc besoin d'être défini soit en tant que chemin UNC, soit avec des lettres de lecteurs mappés.

Remarque : Étant donné que les utilisateurs peuvent changer le mappage des lettres de leurs lecteurs, nous conseillons d'utiliser les chemins UNC dans les règles File Encryption pour des raisons de sécurité.

- **Dossiers hors ligne**

  Si la fonction Windows **Rendre disponible hors connexion** est utilisée, vous n'avez pas à créer de règles spéciales pour les copies (hors ligne) locales des dossiers. Les nouveaux fichiers dans la copie locale du dossier qui a été rendue disponible pour une utilisation hors ligne sont chiffrés d'après la règle pour l'emplacement (réseau) d'origine.

Remarque : retrouvez plus d'informations sur l'appellation des fichiers et des chemins sur http://msdn.microsoft.com/fr-fr/library/aa365247.aspx.

20.1.2 Espaces réservés des chemins dans les règles File Encryption

Les espaces réservés suivants peuvent être utilisés lors de la spécification des chemins dans les règles de chiffrement des stratégies **File Encryption**. Vous pouvez sélectionner ces espaces réservés en cliquant sur le bouton déroulante du champ **Chemin**.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et Mac OS X)	Résultats dans la valeur suivante sur l'ordinateur d'extrémité
<%nom_variable_environnement%>	Tous	Valeur de la variable d'environnement. Exemple : <%NOMUTILISATEUR%>. **Remarque :** si des variables d'environnement contiennent plusieurs emplacements (par exemple, la variable PATH), les chemins ne seront pas divisés en plusieurs règles. Ceci entraîne une erreur et la règle de chiffrement est non valide.
<Poste de travail>	Windows	Dossier virtuel représentant le bureau Microsoft Windows.
<Documents>	Tous	Il s'agit du dossier virtuel représentant l'élément du bureau Mes documents (équivalent à CSIDL_MYDOCUMENTS). Chemin type : C:\Documents and Settings\Nom d'utilisateur\Mes Documents.
<Téléchargements>	Tous	Le dossier dans lequel les téléchargements sont stockés par défaut. Le chemin habituel Windows est C:\Utilisateurs\nom d'utilisateur\Téléchargements.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et Mac OS X)	Résultats dans la valeur suivante sur l'ordinateur d'extrémité
<Musique>	Tous	Répertoire du système de fichiers qui sert de dépôt de données pour les fichiers musique. Chemin type : C:\Documents and Settings\Utilisateur\Mes Documents\Ma Musique.
<Images>	Tous	Répertoire du système de fichiers qui sert de dépôt de données pour les fichiers image. Chemin type : C:\Documents and Settings\nom d'utilisateur\Mes Documents\Mes Images.
<Public>	Tous	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers document de tous les utilisateurs. Chemin type : C:\Utilisateurs\nom d'utilisateur.
<Profil utilisateur>	Tous	Dossier du profil de l'utilisateur. Chemin type : C:\Utilisateurs\nom d'utilisateur. **Remarque :** le chiffrement intégral du profil utilisateur à l'aide de cet espace réservé peut entraîner l'instabilité du bureau Windows sur l'ordinateur d'extrémité.
<Vidéos>	Tous	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers vidéo de tous les utilisateurs. Chemin type : C:\Documents and Settings\All Users\Documents\My Videos.
<Cookies>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les cookies Internet. Chemin type : C:\Documents and Settings\username\Cookies.
<Favorites>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les éléments préférés de l'utilisateur. Chemin type : \Documents and Settings\username\Favorites.
<Local Application Data>	Windows	Répertoire du système de fichiers qui sert de dépôt de données pour les applications locales (non itinérantes). Chemin type : C:\Documents and Settings\username\Local Settings\Application Data.
<Program Data>	Windows	Répertoire du système de fichier contenant les données d'application de tous les

Espace réservé au chemin	Système d'exploitation (Tous=Windows et Mac OS X)	Résultats dans la valeur suivante sur l'ordinateur d'extrémité
		utilisateurs. Chemin type : C:\Documents and Settings\All Users\Application Data.
<Program Files>	Windows	Dossier Program Files. Chemin type : \Program Files. Pour les systèmes 64 bits, celui-ci sera étendu en deux règles : une pour les applications 32 bits et une pour les applications 64 bits.
<Public Music>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers musique de tous les utilisateurs. Chemin type : C:\Documents and Settings\All Users\Documents\My Music.
<Public Pictures>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers image de tous les utilisateurs. Chemin type : C:\Documents and Settings\Tous les utilisateurs\Documents\Mes Images.
<Vidéos publiques>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers vidéo de tous les utilisateurs. Chemin type : C:\Documents and Settings\Tous les utilisateurs\Documents\Mes Vidéos.
<Itinérant>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les données spécifiques aux applications. Chemin type : C:\Documents and Settings\nom d'utilisateur\Application Data.
<Système>	Windows	Dossier système Windows. Chemin type : C:\Windows\System32. Pour les systèmes 64 bits, celui-ci sera étendu en deux règles : une pour le 32 bits et une pour le 64 bits.
<Temporary Burn Folder>	Windows	Répertoire du système de fichiers qui sert de zone de transit pour les fichiers en attente d'écriture sur un CD-ROM. Chemin type : C:\Documents and Settings\username\Local Settings\Application Data\Microsoft\CD Burning.
<Dossier de gravure temporaire>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers temporaires Internet. Chemin type : C:\Documents and Settings\username\Local Settings\Temporary Internet Files.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et Mac OS X)	Résultats dans la valeur suivante sur l'ordinateur d'extrémité
<Windows>	Windows	Répertoire Windows ou SYSROOT. Ceci correspond aux variables d'environnement %windir% ou %SYSTEMROOT%. Chemin type : C:\Windows.
<Amovibles>	Mac OS X	Dirige vers les dossiers racine de tous les supports amovibles Mac OS X.
<Racine>	Mac OS X	Le dossier racine Mac OS X.

Remarque :

Veuillez toujours utiliser les barres obliques inverses pour séparer les chemins même lorsque vous créer des règles File Encryption pour Mac OS X. De cette manière, les règles peuvent être appliquées sur les deux systèmes d'exploitation (Windows et Mac OS X).

Remarque :

Sur le client Mac OS X, les barres obliques inverses vont automatiquement être transformées en barres obliques afin de correspondre aux conditions requises du système d'exploitation Mac OS X.

Toutes erreurs dans les espaces réservés sont consignées dans le journal. Les règles de chiffrement File Encryption erronées sont consignées dans le journal, puis ignorées sur l'ordinateur d'extrémité.

Exemple d'une conversion de chemin

Le chemin Windows suivant

<Profil utilisateur>\Dropbox\personnel

est converti sur le Mac en

/Utilisateurs/<Nom d'utilisateur>/Dropbox/personnel

20.2 Configuration des paramètres de chiffrement des fichiers dans les stratégies Paramètres généraux

En plus des règles de chiffrement définies dans les stratégies **File Encryption**, vous pouvez configurer les paramètres **File Encryption** dans des stratégies du type **Paramètres généraux** :

- **Applications fiables**
- **Applications ignorées**
- **Périphériques ignorés**
- **Activer le chiffrement permanent**

20.2.1 Configuration des applications sécurisées et ignorées pour File Encryption

Vous pouvez définir des applications comme sécurisées pour leur accorder l'accès aux fichiers chiffrés. Ceci s'avère utile, par exemple, pour activer le logiciel antivirus afin de contrôler les fichiers chiffrés.

Vous pouvez définir des applications comme ignorées pour les exempter du chiffrement/déchiffrement transparent des fichiers. Par exemple, si vous définissez un programme de sauvegarde comme une application ignorée, les données chiffrées sauvegardées par le programme restent chiffrées.

Remarque : les processus enfants ne seront pas fiables/ignorés.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.
2. Sous **Chiffrement de fichiers**, cliquez sur le bouton déroulant du champ **Applications fiables** ou **Application ignorées**.
3. Dans la zone de liste de l'éditeur, saisissez les applications à définir comme sécurisées/ignorées.
   - Vous pouvez définir plusieurs applications sécurisées/ignorées dans une stratégie. Chaque ligne de la zone de liste de l'éditeur définir une application.
   - Les noms des applications doivent se terminer par .exe.
   - Les noms des applications doivent être indiqués comme des chemins pleinement qualifiés avec informations sur le lecteur/répertoire, par exemple "c:\dir\example.exe". La saisie d'un nom de fichier seulement (par exemple, "exemple.exe") n'est pas suffisante. Pour une meilleure utilisation, la vue sur une ligne de la liste des applications n'affiche que les noms de fichiers séparés par des points-virgules.
   - Les noms d'applications peuvent contenir les mêmes noms d'espaces réservés pour les dossiers d'environnement Windows et variables d'environnement que les règles de chiffrement dans les stratégies File Encryption. Retrouvez une description des espaces réservés disponibles à la section Espaces réservés pour les chemins des règles File Encryption à la page 169.
4. Enregistrez vos modifications.

Remarque : les paramètres de stratégie **Applications fiables** et **Applications ignorées** sont les paramètres de la machine. La stratégie doit donc être attribuée aux machines, pas aux utilisateurs. Sinon, les paramètres ne deviennent pas actifs.

20.2.2 Configuration des périphériques ignorés pour File Encryption

Vous pouvez définir des périphériques comme ignorés pour les exclure du processus de chiffrement des fichiers. Vous pouvez seulement exclure des périphériques entiers.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.

2. Sous **Chiffrement de fichiers**, cliquez sur le bouton déroulant du champ **Périphériques ignorés**.
3. Dans la zone de liste de l'éditeur :

   a) Sélectionnez **Réseau** pour ne pas chiffrer les données du tout sur le réseau.

   b) Saisissez les noms de périphériques requis pour exclure des périphériques donnés du chiffrement. Ceci peut être utile lorsque vous avez besoin d'exclure des systèmes des fournisseurs tiers.

   Remarque : vous pouvez afficher les noms des périphériques en cours d'utilisation dans le système à l'aide d'outils tiers (par exemple, Device Tree d'OSR). SafeGuard Enterprise consigne dans le journal tous les périphériques auxquels il se connecte et vous pouvez afficher une liste des périphériques connectés et ignorés à l'aide des clés de registre. Retrouvez plus d'informations à la section Affichage des périphériques ignorés et connectés pour la configuration File Encryption à la page 174.

   Vous pouvez exclure des lecteurs de disque (réseau) individuels du chiffrement en créant une règle File Encryption dans une stratégie **File Encryption** et en paramétrant le **Mode** de chiffrement sur **Ignorer**. Vous pouvez uniquement appliquer ce paramètre aux lecteurs administrés par Windows et pas aux volumes Mac OS X.

20.2.2.1 Affichage des périphériques ignorés et connectés pour la configuration File Encryption

Pour vous aider à définir les périphériques ignorés, vous pouvez utiliser des clés du registre pour indiquer quels périphériques sont considérés pour le chiffrement (périphériques connectés) et quels sont ceux qui sont ignorés. La liste des périphériques ignorés indique seulement ceux qui sont véritablement disponibles sur l'ordinateur et qui sont ignorés. Si un périphérique est paramétré pour être ignoré dans une stratégie et s'il n'est pas disponible sur l'ordinateur, il n'apparaît pas dans la liste.

Utilisez les clés de registre suivantes pour afficher les périphériques connectés et ignorés :

- **HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\AttachedDevices**
- **HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\IgnoredDevices**

20.2.3 Configuration du chiffrement permanent pour File Encryption

Le contenu des fichiers chiffrés par File Encryption est déchiffré instantanément si l'utilisateur possède la clé requise. Lorsque le contenu est enregistré sous la forme d'un nouveau fichier dans un emplacement qui n'est pas couvert par une règle de chiffrement, le fichier obtenu ne sera pas chiffré.

Avec le chiffrement permanent, les copies des fichiers chiffrés seront chiffrées, même lorsqu'elles sont enregistrées dans un emplacement non couvert par une règle de chiffrement.

Vous pouvez configurer le chiffrement permanent dans des stratégies du type **Paramètres généraux**. Le paramètre de stratégie **Activer le chiffrement permanent** est activé par défaut.

Remarque : si des fichiers sont copiés ou déplacés sur un périphérique ignoré ou dans un dossier auquel s'applique une stratégie avec un mode de chiffrement **Ignorer**, le paramètre **Activer le chiffrement permanent** n'a aucun effet.

20.3 Utilisation de plusieurs stratégies File Encryption

Toutes les règles de chiffrement File Encryption attribuées par des stratégies et activées pour les utilisateurs/ordinateurs à des nœuds différents dans **Utilisateurs et ordinateurs** dans SafeGuard Management Center sont cumulées.

Vous pouvez attribuer une stratégie **File Encryption** au nœud racine qui inclut des règles adaptées à tous les utilisateurs et des stratégies plus spécifiques à des sous-nœuds spécifiques. Toutes les règles de toutes les stratégies attribuées à des utilisateurs/ordinateurs sont cumulées et appliquées sur l'ordinateur d'extrémité.

20.3.1 Stratégies File Encryption dans le RSOP

Si plusieurs stratégies **File Encryption** s'appliquent à un utilisateur/ordinateur, l'onglet **RSOP** (Resulting Set of Policies, série obtenue de stratégies) dans **Utilisateurs et ordinateurs** affiche la somme de toutes les règles de chiffrement File Encryption de toutes les stratégies **File Encryption**. Les règles sont triées dans l'ordre d'évaluation des règles de chiffrement sur l'ordinateur d'extrémité. Retrouvez plus d'informations à la section Évaluation des règles File Encryption sur les ordinateurs d'extrémité à la page 175

La colonne **Nom de la stratégie** indique d'où les règles individuelles proviennent.

Pour les règles en double, la seconde (et la troisième, etc.) règle est marquée d'une icône. Cette icône fournit aussi une infobulle vous informant que la règle sera ignorée sur l'ordinateur d'extrémité car il s'agit du double d'une règle avec une priorité supérieure.

20.4 Évaluation des règles File Encryption sur les ordinateurs d'extrémité

Sur les ordinateurs d'extrémité, les règles File Encryption sont triées d'une telle façon que les emplacements plus spécifiquement définis sont évalués en premier :

- Si deux règles avec les mêmes paramètres **Chemin** et **Étendue** proviennent de stratégies attribuées à des noeuds différents, la règle de la stratégie la plus proche de l'objet utilisateur dans **Utilisateurs et ordinateurs** est appliquée.
- Si deux règles avec les mêmes paramètres **Chemin** et **Étendue** proviennent de stratégies attribuées au même noeud, la règle de la stratégie ayant la priorité la plus élevée est appliquée.
- Les règle absolues sont évaluées avant les règles relatives, par exemple **`c\encrypt`** avant **`encrypt`**. Retrouvez plus d'informations à la section Informations supplémentaires sur la configuration des chemins dans les règles File Encryption à la page 168.
- Les règles avec un chemin contenant plus de sous-répertoires sont évaluées avant celles avec un chemin contenant moins de sous-répertoires.
- Les règles définies avec UNC sont évaluées avant celles avec des informations sur la lettre du lecteur.
- Les règles dont l'option **Seulement ce dossier** est activée sont évaluées avant celles sans cette option.

- Les règles sous le mode **Ignorer** sont évaluées avant celles sous le mode **Chiffrer** ou **Exclure**.
- Les règles sous le mode **Exclure** sont évaluées avant celles sous le mode **Chiffrer** ou Exclure.
- Si deux règles sont identiques en ce qui concerne les critères indiquées, celle qui vient en premier dans l'ordre alphabétique est évaluée avant l'autre.

20.5 Conflit entre les règles File Encryption

Étant donné que plusieurs stratégies File Encryption peuvent être attribuées à un utilisateur/ordinateur, des conflits sont possibles. Deux règles sont considérées comme étant en conflit, si elles ont les mêmes valeurs pour le chemin, le mode et le sous-répertoire, mais si la clé à utiliser est différente. Dans ce cas, la règle issue de la stratégie File Encryption ayant la priorité la plus élevée s'applique. L'autre règle est abandonnée.

20.6 Utilisation de File Share et SafeGuard Data Exchange

SafeGuard Data Exchange est utilisé pour chiffrer des données stockées sur des supports amovibles connectés à un ordinateur afin d'échanger ces données avec d'autres utilisateurs. Le chiffrement de fichiers est utilisé pour SafeGuard Data Exchange.

Si SafeGuard Data Exchange et File Encryption sont installés sur un ordinateur d'extrémité, il peut arriver qu'une stratégie de chiffrement SafeGuard Data Exchange soit définie pour un lecteur présent sur l'ordinateur et que les stratégies File Encryption soient définies pour des dossiers présents sur le même lecteur. Dans ce cas, la stratégie de chiffrement SafeGuard Data Exchange remplace les stratégies **File Encryption**. Les nouveaux fichiers sont chiffrés en fonction de la stratégie de chiffrement de SafeGuard Data Exchange.

Retrouvez plus d'informations sur SafeGuard Data Exchange à la section SafeGuard Data Exchange à la page 177.

21 SafeGuard Data Exchange

SafeGuard Data Exchange est utilisé pour chiffrer des données stockées sur des supports amovibles connectés à un ordinateur afin d'échanger ces données avec d'autres utilisateurs. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale.

Seuls les utilisateurs disposant des clés appropriées peuvent lire le contenu des données chiffrées. Tout processus de chiffrement ultérieur est exécuté de manière transparente.

Dans le cadre d'une administration centralisée, vous définissez la gestion des données de supports amovibles.

En tant que responsable de la sécurité, vous définissez les paramètres spécifiques dans une stratégie du type **Protection des périphériques** avec **Supports amovibles** comme **Cible de protection de périphérique**.

Le chiffrement basé sur fichier doit être utilisé pour SafeGuard Data Exchange.

21.1 Clés de groupe

Pour échanger des données chiffrées entre utilisateurs, des clés de groupe SafeGuard Enterprise doivent être utilisées. Si la clé de groupe se trouve dans les jeux de clés des utilisateurs, ces derniers peuvent accéder en toute transparence aux supports amovibles connectés à leurs ordinateurs.

Sur les ordinateurs sur lesquels SafeGuard Enterprise n'est pas installé, il est impossible d'accéder aux données chiffrées de supports amovibles, à l'exception de la clé de domaine/groupe définie de manière centralisée qui peut être utilisée avec la phrase secrète des supports.

Remarque : safeguard Portable peut être utilisé pour utiliser/partager des données chiffrées de supports amovibles sur/avec des ordinateurs/utilisateurs ne disposant pas de SafeGuard Enterprise. SafeGuard Portable nécessite l'utilisation de clés locales ou d'une phrase secrète des supports.

21.2 Clés locales

SafeGuard Data Exchange prend en charge le chiffrement à l'aide de clés locales. Des clés locales sont créées sur les ordinateurs et peuvent être utilisées pour chiffrer des données de supports amovibles. Elles sont créées en saisissant une phrase secrète et sauvegardées dans la base de données de SafeGuard Enterprise.

Remarque : par défaut, l'utilisateur est autorisé à créer des clés locales. Si des utilisateurs n'y sont pas autorisés, vous devez désactiver cette option de manière explicite. Ceci doit être effectué dans une stratégie de type **Protection des périphériques** avec **Périphériques de stockage locaux** comme **Cible de protection de périphérique** (**Paramètres généraux** > **L'utilisateur est autorisé à créer une clé locale** > **Non**).

Si des clés locales sont utilisées pour chiffrer des fichiers sur des supports amovibles, ces fichiers peuvent être déchiffrés à l'aide de SafeGuard Portable sur un ordinateur sur lequel SafeGuard

Data Exchange n'est pas installé. À l'ouverture des fichiers avec SafeGuard Portable, l'utilisateur est invité à saisir la phrase secrète spécifiée lors de la création de la clé. L'utilisateur peut ouvrir le fichier s'il connaît la phrase secrète.

Grâce à SafeGuard Portable, chaque utilisateur connaissant la phrase secrète peut accéder à un fichier chiffré sur un support amovible. Il est ainsi également possible de partager des données chiffrées avec des partenaires ne disposant pas de SafeGuard Enterprise. SafeGuard Portable et la phrase secrète des fichiers auxquels ils doivent accéder doivent leur être fournis.

Si différentes clés locales sont utilisées pour chiffrer des fichiers de supports amovibles, vous pouvez également restreindre l'accès aux fichiers. Par exemple : vous chiffrez les fichiers contenus sur une carte mémoire USB à l'aide d'une clé avec la phrase secrète *ma_clélocale* et chiffrez un fichier nommé *PourMonPartenaire.doc* à l'aide de la phrase secrète *partenaire_clélocale*. Si vous donnez la carte USB à un partenaire et fournissez la phrase secrète*partenaire_clélocale* à ce dernier, il n'aura accès qu'au fichier *PourMonPartenaire.doc*.

Remarque : par défaut, SafeGuard Portable est copié automatiquement sur les supports amovibles connectés au système dès l'écriture de contenu sur les supports couverts par une règle de chiffrement. Si vous ne souhaitez pas que SafeGuard Portable soit copié sur les supports amovibles, désactivez l'option **Copier SG Portable sur la cible** dans une stratégie du type **Chiffrement de périphérique**.

21.3 Phrase secrète des supports

SafeGuard Data Exchange vous permet de spécifier qu'une seule phrase secrète des supports pour tous les supports amovibles (sauf les supports optiques) doit être créée sur les ordinateurs d'extrémité. La phrase secrète des supports permet d'accéder à la clé de domaine/groupe définie de manière centralisée et à toutes les clés locales utilisées dans SafeGuard Portable. L'utilisateur ne saisit qu'une seule phrase secrète et peut accéder à tous les fichiers chiffrés dans SafeGuard Portable, quelle que soit la clé locale utilisée pour le chiffrement.

Sur chaque ordinateur d'extrémité et pour chaque périphérique, une clé de chiffrement de support unique pour le chiffrement de données est créée automatiquement. Cette clé est protégée par la phrase secrète des supports et une clé de domaine/groupe définie de manière centralisée. Sur un ordinateur sur lequel SafeGuard Data Exchange est installé, il n'est donc pas nécessaire de saisir la phrase secrète des supports pour accéder aux fichiers chiffrés contenus sur le support amovible. L'accès est accordé automatiquement si la clé appropriée se trouve dans le jeu de clés de l'utilisateur.

La clé de domaine/groupe à utiliser doit être spécifiée sous **Clé définie pour le chiffrement**.

La fonction de phrase secrète des supports est disponible lorsque l'option **L'utilisateur peut définir une phrase secrète des supports pour les périphériques** est activée dans une stratégie de type **Protection des périphériques**.

Lorsque ce paramètre est activé sur l'ordinateur, l'utilisateur est invité automatiquement à saisir une phrase secrète des supports lorsqu'il connecte des supports amovibles pour la première fois. La phrase secrète des supports est valide sur chaque ordinateur auquel l'utilisateur peut se connecter. L'utilisateur peut également changer la phrase secrète des supports. La synchronisation est alors automatique lorsque la phrase secrète reconnue sur l'ordinateur et la phrase secrète des supports amovibles ne correspondent pas.

En cas d'oubli de la phrase secrète des supports l'utilisateur peut la récupérer sans recourir au support.

Remarque : pour activer la phrase secrète des supports, activez l'option **L'utilisateur peut définir une phrase secrète des supports pour les périphériques** dans une stratégie de type **Chiffrement de périphérique**. Cette option n'est disponible que si vous avez sélectionné **Supports amovibles** comme **Cible de protection de périphérique**.

21.3.1 Phrase secrète des supports et ordinateurs d'extrémité non administrés

Sur un ordinateur d'extrémité non administré, autrement dit un ordinateur fonctionnant en mode autonome, sur lequel la fonction de phrase secrète des supports est désactivée, aucune clé n'est disponible une fois l'installation terminée, car les ordinateurs d'extrémité non administrés utilisent des clés locales uniquement. Avant de pouvoir utiliser le chiffrement, l'utilisateur doit créer une clé.

Si la fonction de phrase secrète des supports est activée dans une stratégie de support amovible pour ces ordinateurs, la clé de chiffrement de support est créée automatiquement sur l'ordinateur client et peut être utilisée pour un chiffrement immédiatement après l'installation. Il s'agit d'une clé prédéfinie du jeu de clés de l'utilisateur qui s'affiche sous la forme d'un <nom utilisateur> dans les boîtes de dialogue de sélection de clé.

Le cas échéant, les clés de chiffrement de support sont également utilisées pour toutes les tâches de chiffrement initial.

21.4 Bon usage

Cette section décrit des études de cas classiques de SafeGuard Data Exchange et comment les mettre en œuvre en créant les stratégies appropriées.

Bob et Alice sont deux employés de la même société et disposent de SafeGuard Data Exchange. Joe est un partenaire externe et ne dispose pas de SafeGuard Enterprise sur son ordinateur.

21.4.1 Utilisation interne uniquement

Bob souhaite partager des données chiffrées sur un support amovible avec Alice. Ils font partie du même groupe et disposent donc de la clé de groupe appropriée dans leur jeu de clés SafeGuard Enterprise. Étant donné qu'ils utilisent la même clé de groupe, ils peuvent accéder en toute transparence aux fichiers chiffrés sans saisir de phrase secrète.

Vous devez définir les paramètres dans une stratégie de type **Protection du périphérique\Supports amovibles** :

- **Mode de chiffrement du support : Basé sur fichier**
- **Clé à utiliser pour le chiffrement : Clé définie dans la liste**
  - Clé définie dans la liste : <clé de groupe/domaine > (par exemple, groupe_utilisateurs_Bob_Alice@DC=...) pour s'assurer qu'ils partagent la même clé

Si les stratégies de l'entreprise stipulent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers : Oui**

  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.

- **L'utilisateur peut annuler le chiffrement initial : Non**

  L'utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.

- **L'utilisateur n'est pas autorisé à accéder aux fichiers non chiffrés : Non**

  Si des fichiers au format brut sont détectés sur le support amovible, leur accès est refusé.

- **L'utilisateur peut déchiffrer des fichiers : Non**

  L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.

- **Copier portable SG sur la cible : Non**

  SafeGuard Portable n'est pas nécessaire tant que les données de supports amovibles sont partagées dans un groupe de travail. SafeGuard Portable permet également d'autoriser le déchiffrement de fichiers sur des ordinateurs sur lesquels SafeGuard Enterprise n'est pas installé.

Les utilisateurs peuvent partager des données en échangeant simplement leurs périphériques. Lorsqu'ils connectent les périphériques à leurs ordinateurs, ils accèdent en toute transparence aux fichiers chiffrés.

Remarque : cette étude de cas est possible grâce à la fonction de chiffrement de périphérique de SafeGuard Enterprise dans laquelle l'ensemble du périphérique amovible est chiffré par secteur.

21.4.2 Utilisation à domicile ou personnelle sur des ordinateurs tiers

- **À domicile :**

  Bob souhaite utiliser son support amovible chiffré sur son PC personnel, sur lequel SafeGuard Enterprise n'est pas installé. Sur son ordinateur personnel, Bob déchiffre les fichiers avec SafeGuard Portable. En définissant une phrase secrète des supports pour tous les supports amovibles de Bob, il ouvre simplement SafeGuard Portable et saisit la phrase secrète du support. Il a ensuite accès de manière transparente à tous les fichiers chiffrés, quelle que soit la clé locale utilisée pour les chiffrer.

- **Utilisation personnelle sur des ordinateurs tiers :**

  Bob connecte le périphérique amovible à l'ordinateur de Joe (partenaire externe) et saisit la phrase secrète des supports pour accéder aux fichiers chiffrés stockés sur le périphérique. Bob peut alors copier les fichiers (chiffrés ou non) sur l'ordinateur de Joe.

Comportement sur l'ordinateur d'extrémité :

- Bob connecte pour la première fois le périphérique amovible.

- La clé de chiffrement de support, unique à chaque périphérique, est créée automatiquement.
- Bob est invité à saisir la phrase secrète des supports pour l'utiliser hors ligne via SafeGuard Portable.
- L'utilisateur n'a pas besoin de connaître les clés utilisées ou le jeu de clés. La clé de chiffrement de support est toujours utilisée pour le chiffrement de données sans aucune interaction de l'utilisateur. La clé de chiffrement de support n'est pas visible, y compris pour l'utilisateur. Seule la clé de groupe/domaine définie de manière centralisée est visible.
- Bob et Alice, du même groupe ou domaine, accèdent de manière transparente car ils partagent la même clé de groupe/domaine.
- Si Bob souhaite accéder à des fichiers chiffrés d'un périphérique amovible sur un ordinateur sur lequel SafeGuard Data Exchange n'est pas installé, il peut utiliser la phrase secrète des supports dans SafeGuard Portable.

Vous devez définir les paramètres dans une stratégie de type **Protection des périphériques\Supports amovibles** :

- **Mode de chiffrement du support : Basé sur fichier**
- **Clé à utiliser pour le chiffrement : Clé définie dans la liste**

  Clé définie dans la liste : <clé de groupe/domaine > (par exemple, groupe_utilisateurs_Bob_Alice@DC=...) pour s'assurer qu'ils partagent la même clé

- **L'utilisateur peut définir une phrase secrète des supports pour les périphériques : Oui**

  L'utilisateur définit une phrase secrète des supports sur son ordinateur qui s'applique à tous les supports amovibles.

- **Copier portable SG sur la cible : Oui**

  SafeGuard Portable permet à l'utilisateur d'accéder à tous les fichiers chiffrés du support amovible en saisissant une phrase secrète des supports unique sur un système sur lequel SafeGuard Data Exchange n'est pas installé.

Si les stratégies de l'entreprise définissent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers : Oui**

  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.

- **L'utilisateur peut annuler le chiffrement initial : Non**

  L'utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.

- **L'utilisateur n'est pas autorisé à accéder aux fichiers non chiffrés : Non**

  Si des fichiers au format brut sont détectés sur le support amovible, leur accès est refusé.

- **L'utilisateur peut déchiffrer des fichiers : Non**

  L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.

Au bureau, Bob et Alice accèdent de manière transparente aux fichiers chiffrés du support amovible. À domicile ou sur les ordinateurs tiers, ils peuvent utiliser SafeGuard Portable pour ouvrir des fichiers chiffrés. Les utilisateurs saisissent seulement la phrase secrète des supports et peuvent accéder à tous les fichiers chiffrés. Cette méthode simple mais fiable permet de chiffrer des données sur tous les supports amovibles. Cette configuration vise à réduire au maximum l'interaction de l'utilisateur tout en chiffrant chaque fichier d'un support amovible et en permettant aux utilisateurs d'accéder hors ligne aux fichiers chiffrés. L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.

Remarque : dans cette configuration, les utilisateurs ne sont pas autorisés à créer des clés locales car elles sont inutiles dans ce cas de figure. Ceci doit être spécifié dans une stratégie du type **Protection des périphériques** avec **Périphériques de stockage locaux** comme **Cible de protection de périphérique** (**Paramètres généraux** > **L'utilisateur est autorisé à créer une clé locale** > **Non**).

- **Copier SG Portable vers support amovible : Numéro**

  SafeGuard Portable n'est pas nécessaire tant que les données de supports amovibles sont partagées dans un groupe de travail. SafeGuard Portable permet également d'autoriser le déchiffrement de fichiers sur des ordinateurs sur lesquels SafeGuard Enterprise n'est pas installé.

Au bureau, l'utilisateur accède de manière transparente aux fichiers chiffrés d'un support amovible. À son domicile, il utilise SafeGuard Portable pour ouvrir des fichiers chiffrés. L'utilisateur saisit simplement la phrase secrète des supports et accède à tous les fichiers chiffrés, quelle que soit la clé de chiffrement utilisée.

21.4.3 Partage d'un support amovible avec un tiers externe

Remarque : cet exemple s'applique uniquement aux ordinateurs d'extrémité Windows.

Bob souhaite partager un périphérique chiffré avec Joe (tiers externe) qui ne dispose pas de SafeGuard Data Exchange et qui doit donc utiliser SafeGuard Portable. Si on suppose que Bob ne souhaite pas que Joe accède à tous les fichiers chiffrés du support amovible, il peut créer une clé locale et chiffrer les fichiers avec cette clé. Joe peut alors utiliser SafeGuard Portable et ouvrir les fichiers chiffrés à l'aide de la phrase secrète de la clé locale et Bob peut toujours utiliser la phrase secrète des supports pour accéder aux fichiers chiffrés du support amovible.

Comportement sur l'ordinateur

- Bob connecte pour la première fois le périphérique amovible. La clé de chiffrement de support, unique à chaque périphérique, est créée automatiquement.
- Bob est invité à saisir la phrase secrète des supports pour l'utiliser hors ligne.
- La clé de chiffrement de support est utilisée pour le chiffrement de données sans aucune intervention de l'utilisateur, mais...
- Bob peut maintenant créer ou sélectionner une clé locale (par exemple, JoeClé) pour chiffrer des fichiers spécifiques à échanger avec Joe.
- Bob et Alice, du même groupe ou domaine, accèdent de manière transparente car ils partagent la même clé de groupe/domaine.

- Si Bob souhaite accéder à des fichiers chiffrés d'un périphérique amovible sur un ordinateur sur lequel SafeGuard Data Exchange n'est pas installé, il peut utiliser la phrase secrète des supports dans SafeGuard Portable.
- Joe peut accéder aux fichiers spécifiques en saisissant la phrase secrète de la clé (JoeClé) sans accéder à l'ensemble des fichiers du support amovible.

Vous devez définir les paramètres dans une stratégie du type **Protection des périphériques\Supports amovibles** :

- **Mode de chiffrement du support : Basé sur fichier**
- **Clé à utiliser pour le chiffrement : Toute clé du jeu de clés utilisateur**

  Permet à l'utilisateur de choisir différentes clés pour chiffrer des fichiers de son support amovible.

  > **Clé définie pour le chiffrement :** <clé de groupe/domaine> (par exemple groupe_utilisateurs_Bob_Alice@DC=...) L'utilisateur peut partager des données dans son groupe de travail et permettre à un autre utilisateur d'accéder de manière transparente au support amovible lorsqu'il le connecte à son ordinateur professionnel.

- **L'utilisateur peut définir une phrase secrète des supports pour les périphériques : Oui**

  L'utilisateur définit une phrase secrète des supports sur son ordinateur qui s'applique à tous les supports amovibles.

- **Copier portable SG sur la cible : Oui**

  SafeGuard Portable permet à l'utilisateur d'accéder à tous les fichiers chiffrés du support amovible en saisissant une phrase secrète des supports unique sur un système sur lequel SafeGuard Data Exchange n'est pas installé.

Si les stratégies de l'entreprise définissent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers : Oui**

  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.

- **L'utilisateur peut annuler le chiffrement initial : Non**

  L'utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.

- **L'utilisateur n'est pas autorisé à accéder aux fichiers non chiffrés : Non**

  Si des fichiers au format brut sont détectés sur le support amovible, leur accès est refusé.

- **L'utilisateur peut déchiffrer des fichiers : Non**

  L'utilisateur n'est pas autorisé à déchiffrer des fichiers de supports amovibles.

Au bureau, Bob et Alice accèdent de manière transparente aux fichiers chiffrés du support amovible. À leur domicile, ils peuvent utiliser SafeGuard Portable pour ouvrir des fichiers chiffrés en saisissant la phrase secrète des supports. Si Bob ou Alice souhaite partager le support

amovible sur un ordinateur tiers sur lequel SafeGuard Data Exchange n'est pas installé, ils peuvent utiliser des clés locales pour s'assurer que le tiers externe n'accède qu'à certains fichiers. Cette configuration avancée implique une interaction plus importante de l'utilisateur en l'autorisant à créer des clés locales sur son ordinateur.

Remarque : pour ce faire, l'utilisateur doit au préalable être autorisé à créer des clés locales (paramètre par défaut dans SafeGuard Enterprise).

21.5 Configuration des applications fiables et ignorées pour SafeGuard Data Exchange

Vous pouvez définir des applications comme fiables pour leur accorder l'accès aux fichiers chiffrés. C'est par exemple nécessaire pour activer le logiciel antivirus afin de contrôler les fichiers chiffrés.

Vous pouvez définir des applications comme ignorés pour les exempter du chiffrement/déchiffrement transparent des fichiers. Par exemple, si vous définissez un programme de sauvegarde comme une application ignorée, les données chiffrées sauvegardées par le programme restent chiffrées.

Remarque : les processus enfants ne seront pas fiables/ignorés.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.
2. Sous **Chiffrement de fichiers**, cliquez sur le bouton déroulant du champ **Applications fiables** ou **Application ignorées**.
3. Dans la zone de liste de l'éditeur, saisissez les applications à définir comme fiables/ignorées.
   - Vous pouvez définir plusieurs applications fiables/ignorées dans une stratégie. Chaque ligne de la zone de liste de l'éditeur définir une application.
   - Les noms des applications doivent se terminer par .exe.
   - Les noms des applications doivent être spécifiés comme des chemins pleinement qualifiés avec informations sur le lecteur/répertoire. La saisie d'un nom de fichier seulement (par exemple, "exemple.exe") n'est pas suffisante. Pour une meilleure utilisation, la vue sur une ligne de la liste des applications n'affiche que les noms de fichiers séparés par des points-virgules.
4. Enregistrez vos modifications.

Remarque : les paramètres de stratégie **Applications fiables** et **Applications ignorées** sont les paramètres machine. La stratégie doit donc être attribuée aux machines, pas aux utilisateurs. Sinon, les paramètres ne deviennent pas actifs.

21.6 Configuration des périphériques ignorés pour SafeGuard Data Exchange

Vous pouvez définir des périphériques comme ignorés pour les exclure du processus de chiffrement des fichiers. Vous pouvez seulement exclure des périphériques entiers.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.
2. Sous **Chiffrement de fichiers**, cliquez sur le bouton déroulant du champ **Périphériques ignorés**.
3. Dans la zone de liste de l'éditeur, saisissez les noms de périphériques requis pour exclure des périphériques donnés du chiffrement. Ceci peut être utile lorsque vous avez besoin d'exclure des systèmes des fournisseurs tiers.

   Remarque : vous pouvez afficher les noms des périphériques en cours d'utilisation dans le système à l'aide d'outils tiers (par exemple, Device Tree d'OSR). SafeGuard Enterprise consigne dans le journal tous les périphériques auxquels il se connecte et vous pouvez afficher une liste des périphériques connectés et ignorés à l'aide des clés de registre.

21.6.1 Affichage des périphériques connectés et ignorés pour la configuration de SafeGuard Data Exchange

Pour vous aider à définir les périphériques ignorés, vous pouvez utiliser des clés du registre pour indiquer quels périphériques sont considérés pour le chiffrement (périphériques connectés) et quels sont ceux qui sont ignorés. La liste des périphériques ignorés indique seulement ceux qui sont véritablement disponibles sur l'ordinateur et qui sont ignorés. Si un périphérique est paramétré pour être ignoré dans une stratégie et s'il n'est pas disponible sur l'ordinateur, il n'apparaît pas dans la liste.

Utilisez les clés de registre suivantes pour afficher les périphériques connectés et ignorés :

- **`HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\AttachedDevices`**
- **`HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\IgnoredDevices`**

21.7 Configuration du chiffrement permanent pour SafeGuard Data Exchange

Le contenu des fichiers chiffrés par SafeGuard Data Exchange est déchiffré à la volée, si l'utilisateur possède la clé requise. Lorsque le contenu est enregistré sous la forme d'un nouveau fichier dans un emplacement qui n'est pas couvert par une règle de chiffrement, le fichier obtenu ne sera pas chiffré.

Avec le chiffrement permanent, les copies des fichiers chiffrés seront chiffrées, même lorsqu'elles sont enregistrées dans un emplacement non couvert par une règle de chiffrement.

Vous pouvez configurer le chiffrement permanent dans des stratégies du type **Paramètres généraux**. Le paramètre de stratégie **Activer le chiffrement permanent** est activé par défaut.

Remarque :

- Si des fichiers sont copiés ou déplacés sur un périphérique ignoré ou dans un dossier auquel s'applique une stratégie avec un **Mode** de chiffrement **Ignorer**, le paramètre **Activer le chiffrement permanent** n'a aucun effet.
- Les opérations de copie sont détectées d'après les noms de fichiers. Lorsqu'un utilisateur enregistre un fichier chiffré avec **Enregistrer sous** sous un nom de fichier différent dans un emplacement non couvert par une règle de chiffrement, le fichier sera en texte brut.

21.8 Suivi de fichiers sur supports amovibles

Vous pouvez réaliser un suivi des fichiers accessibles sur les supports amovibles à l'aide de la fonction **Rapports** du SafeGuard Management Center. L'accès aux fichiers peut faire l'objet d'un suivi quelle que soit la stratégie de chiffrement applicable aux fichiers présents sur les supports amovibles.

Dans une stratégie de type **Journalisation**, vous pouvez définir ce qui suit :

- Un événement à consigner dans le journal lorsqu'un fichier ou un répertoire est créé sur un périphérique amovible.
- Un événement à consigner dans le journal lorsqu'un fichier ou un répertoire est renommé sur un périphérique amovible.
- Un événement à consigner dans le journal lorsqu'un fichier ou un répertoire est supprimé d'un périphérique amovible.

Retrouvez plus d'informations à la section Rapport d'accès aux fichiers pour les supports amovibles à la page 259.

21.9 SafeGuard Data Exchange et File Share

Le module File Share de SafeGuard Enterprise permet un chiffrement basé sur fichier sur les emplacements réseau, surtout pour les groupes de travail et les partages réseau.

Si SafeGuard Data Exchange et File Share sont installés sur un ordinateur d'extrémité, il peut arriver qu'une stratégie de chiffrement SafeGuard Data Exchange soit définie pour un lecteur présent sur l'ordinateur et que les stratégies File Encryption soient définies pour des dossiers présents sur le même lecteur. Si c'est le cas, la stratégie de chiffrement SafeGuard Data Exchange remplace les stratégies File Encryption. Les nouveaux fichiers sont chiffrés en fonction de la stratégie de chiffrement de SafeGuard Data Exchange.

Retrouvez plus d'informations sur File Share à la section Utilisation de File Encryption avec File Share à la page 165.

22 Cloud Storage

Le module Cloud Storage de SafeGuard Enterprise offre le chiffrement de fichiers des données stockées dans le Cloud.

Cela ne change pas la façon dont les utilisateurs exploitent les données stockées dans le Cloud. Les utilisateurs utilisent toujours les mêmes applications de synchronisation spécifiques aux fournisseurs pour envoyer des données au Cloud ou en recevoir depuis celui-ci. Le but de Cloud Storage est de s'assurer que les copies locales des données stockées dans le Cloud sont chiffrées de manière transparente et qu'elles seront donc toujours stockées dans le Cloud sous une forme chiffrée.

Dans SafeGuard Management Center, créez des **Définitions Cloud Storage** (**CSD, Cloud Storage Definitions**) et utilisez-les dans les stratégies **Protection des périphériques**. Les définitions Cloud Storage prédéfinies de différents fournisseurs de stockage dans le Cloud sont disponibles. Par exemple, Dropbox ou Egnyte.

Après attribution d'une stratégie Cloud Storage aux ordinateurs d'extrémité, les fichiers présents dans les emplacements couverts par la stratégie sont chiffrés de manière transparente sans interaction avec l'utilisateur :

- Les fichiers chiffrés seront synchronisés dans le Cloud.
- Les fichiers chiffrés reçus du Cloud peuvent comme d'habitude être modifiés par les applications.

Pour accéder aux fichiers chiffrés Cloud Storage sur les ordinateurs d'extrémité sans Cloud Storage de SafeGuard Enterprise, SafeGuard Portable peut être utilisé pour lire les fichiers chiffrés.

Remarque : cloud Storage chiffre uniquement les nouvelles données stockées dans le Cloud. Si les données sont déjà stockées dans le Cloud avant l'installation de Cloud Storage, ces données ne seront pas automatiquement chiffrées. Si vous voulez chiffrer ces données, vous devez les supprimer du Cloud, puis les saisir de nouveau après installation de Cloud Storage.

22.1 Conditions requises pour le logiciel de Cloud Storage

Pour activer le chiffrement des données stockées dans le Cloud, le logiciel fourni par le fournisseur de Stockage dans le Cloud :

- Doit fonctionner sur l'ordinateur sur lequel Cloud Storage est installé.
- Doit avoir une application (ou un service système) stockée dans le système de fichiers local et synchroniser les données entre le Cloud et le système local.
- Doit stocker les données synchronisées dans le système de fichiers local.

22.2 Création de définitions Cloud Storage (CSD)

Dans SafeGuard Management Center, les définitions Cloud Storage prédéfinies de différents fournisseurs de stockage dans le Cloud sont disponibles. Par exemple, Dropbox ou Egnyte.

Vous pouvez modifier les chemins définis dans les définitions Cloud Storage prédéfinies selon vos besoins ou créer une nouvelle définition à partir des valeurs d'une définition prédéfinie. Ceci s'avère particulièrement utile, par exemple, si vous souhaitez uniquement chiffrer une partie des données de votre stockage dans le Cloud. Vous pouvez également créer vos propres définitions Cloud Storage.

Remarque : lorsqu'ils sont chiffrés, certains dossiers (par exemple, le dossier d'installation Dropbox) peut empêcher l'exécution du système d'exploitation ou d'applications. Lorsque vous créez des définitions Cloud Storage pour les stratégies de **Protection des périphériques**, assurez-vous que ces dossiers ne sont pas chiffrés.

1. Dans la zone de navigation **Stratégies**, sélectionnez **Définitions Cloud Storage**.
2. Dans le menu contextuel **Définitions Cloud Storage**, cliquez sur **Nouvelle** > **Définition Cloud Storage**.
3. La boîte de dialogue **Nouvelle définition Cloud Storage** apparaît. Saisissez un nom de définition Cloud Storage.
4. Cliquez sur **OK**. La définition Cloud Storage apparaît avec le nom saisi sous le nœud racine **Définitions Cloud Storage** dans la zone de navigation **Stratégies**.
5. Sélectionnez la définition Cloud Storage. Dans la zone de travail à droite, le contenu d'une définition Cloud Storage apparaît :

   - **Nom de la cible :**

     Il s'agit du nom que vous avez saisi initialement. Il sert à référencer la définition Cloud Storage comme cible dans une stratégie de type **Protection des périphériques**.
   - **Application de synchronisation :**

     Saisissez le chemin et l'application qui synchronise les données avec le Cloud (par exemple : <Bureau>\dropbox\dropbox.exe). L'application doit résider sur un lecteur local.
   - **Dossier de synchronisation :**

     Saisissez le ou les dossiers qui seront synchronisés avec le Cloud. Seuls les chemins locaux sont pris en charge.

     Remarque : pour les chemins dans les paramètres **Application de synchronisation** et **Dossier de synchronisation**, les mêmes espaces réservés que pour **File Encryption** sont pris en charge. Retrouvez plus d'informations à la section Espaces réservés pour les chemins dans les règles de chiffrement File Encryption à la page 169.

22.2.1 Espaces réservés pour les fournisseurs de stockage dans le Cloud

En tant que responsable de la sécurité, vous pouvez utiliser des espaces réservés pour les fournisseurs du stockage dans le Cloud afin de définir des applications de synchronisation et des dossiers de synchronisation. Ces espaces réservés représentent les applications tierces de stockage dans le Cloud prises en charge. Vous pouvez utiliser l'espace réservé pour spécifier une certaine application tierce comme application de synchronisation et même utiliser le même espace réservé pour qu'il pointe vers les dossiers de synchronisation que l'application tierce utilise véritablement pour la synchronisation.

Les espaces réservés pour le fournisseur de stockage dans le Cloud sont encapsulés par `<!` et `!>`.

Espaces réservés actuellement pris en charge :

Fournisseur	Espace réservé	Utilisable dans le paramètre CSD	Résultat
Dropbox	**`<!Dropbox!>`**	**Application de synchronisation, Dossiers de synchronisation**	Pour les applications de synchronisation : Le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Dropbox. Pour les dossiers de synchronisation : Le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel Dropbox.
Egnyte	**`<!Egnyte!>`**	**Application de synchronisation**	Le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Egnyte.
	`<!EgnytePrivate!>`	**Dossiers de synchronisation**	Tous les dossiers confidentiels du stockage Cloud d'Egnyte. Pour les utilisateurs Egnyte classiques, il s'agit généralement d'un seul dossier. Pour les administrateurs Egnyte, cet espace réservé consiste généralement en plusieurs dossiers.
	`<!EgnyteShared!>`	**Dossiers de synchronisation**	Tous les dossiers partagés du stockage Cloud d'Egnyte.
	Remarque : Les modifications de la structure du dossier Egnyte (y compris, l'ajout ou la suppression de dossiers confidentiels ou partagés) sont détectées automatiquement. Les stratégies affectées sont mises à jour automatiquement.		

Fournisseur	Espace réservé	Utilisable dans le paramètre CSD	Résultat
	Remarque : les dossiers de synchronisation peuvent se trouver sur des emplacements du réseau. Vous pouvez donc saisir les chemins réseau dans le paramètre **Dossiers de synchronisation**. Le module Cloud Storage de SafeGuard Enterprise se connecte donc par défaut aux systèmes de fichiers réseau. Si cette opération n'est pas nécessaire, vous pouvez désactiver ce comportement en définissant une stratégie **Paramètres généraux** et en sélectionnant **Réseau** sous **Périphériques ignorés**.		
Google Drive	**<!GoogleDrive!>**	**Application de synchronisation, Dossiers de synchronisation**	Pour les applications de synchronisation : Le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Google Drive. Pour les dossiers de synchronisation : Le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel Google Drive.
SkyDrive	**<!SkyDrive!>**	**Application de synchronisation, Dossiers de synchronisation**	Pour les applications de synchronisation : Le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel SkyDrive. Pour les dossiers de synchronisation : Le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel SkyDrive.
Media Center	**<!Mediacenter!>**	**Application de synchronisation, Dossiers de synchronisation**	Pour les applications de synchronisation : Le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Media Center. Pour les dossiers de synchronisation : Le chemin pleinement

Fournisseur	Espace réservé	Utilisable dans le paramètre CSD	Résultat
			qualifié du dossier de synchronisation utilisé par le logiciel Media Center.

Exemple

Si vous utilisez Dropbox comme fournisseur de stockage dans le Cloud, vous pouvez simplement saisir **<!Dropbox!>** dans **Application de synchronisation**. Si vous n'indiquez pas explicitement de dossier de synchronisation, **<!Dropbox!>** est aussi copié dans la liste des dossiers sous **Dossiers de synchronisation**.

En supposant que

- Vous avez utilisé les espaces réservés <!Dropbox!> comme application de synchronisation et <!Dropbox!>\encrypt comme dossier de synchronisation dans la définition Cloud Storage (CSD, Cloud Storage Definition)
- Dropbox est installé sur l'ordinateur d'extrémité
- L'utilisateur dispose de d:\dropbox configuré en tant que dossier à synchroniser avec Dropbox :

Lorsque l'ordinateur d'extrémité SafeGuard Enterprise reçoit une stratégie avec une CSD comme celle-ci, il interprète automatiquement les espaces réservés de la CSD pour qu'ils correspondent au chemin de Dropbox.exe pour l'application de synchronisation, puis il lit la configuration Dropbox et définit la stratégie de chiffrement dans le dossier d:\dropbox\encrypt.

22.2.2 Exportation et importation des définitions Cloud Storage

En tant que responsable de la sécurité, vous pouvez exporter et importer des définitions Cloud Storage (CSD, Cloud Storage Definitions). Une CSD sera exportée sous la forme d'un fichier XML.

- Pour exporter une CSD, cliquez sur **Exporter une définition de Cloud Storage...** dans le menu contextuel de la définition Cloud Storage désirée dans la zone **Stratégie**.
- Pour importer une CSD, cliquez sur **Importer une définition de Cloud Storage...** dans le menu contextuel du nœud de la définition Cloud Storage dans la zone **Stratégie**.

Les deux commandes sont également disponibles dans le menu **Actions** du SafeGuard Management Center.

22.3 Création d'une stratégie de protection des périphériques avec une définition Cloud Storage

Des définitions Cloud Storage doivent avoir été créées auparavant. Les définitions Cloud Storage prédéfinies de différents fournisseurs de stockage dans le Cloud sont disponibles. Par exemple, Dropbox ou Egnyte.

Vous définissez les paramètres pour chiffrer les données de stockage dans le Cloud dans une stratégie du type **Protection des périphériques**.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Protection des périphériques**.
2. Sélectionnez une définition Cloud Storage comme cible.
3. Cliquez sur **OK**. La nouvelle stratégie s'affiche dans la fenêtre de navigation sous **Éléments de stratégie**. Dans la zone d'action, tous les paramètres de la stratégie **Protection du périphérique** s'affichent et peuvent être changés.
4. Pour le **Mode de chiffrement du support**, sélectionnez **Basé sur fichier**. Le chiffrement basé sur volume n'est pas pris en charge.
5. Sous **Algorithme à utiliser pour le chiffrement**, sélectionnez l'algorithme à utiliser pour le chiffrement des données dans les dossiers de synchronisation définis dans la CSD.
6. Les paramètres **Clé à utiliser pour le chiffrement** et **Clé définie pour le chiffrement** servent à définir la clé ou les clés qui seront utilisées pour le chiffrement. Retrouvez plus d'informations à la section Protection des périphériques à la page 135.
7. Si vous activez le paramètre **Copier SG Portable sur la cible**, SafeGuard Portable est copié dans chaque dossier de synchronisation à chaque fois que du contenu est écrit. SafeGuard Portable est une application qui peut être utilisée pour lire les fichiers chiffrés sur les ordinateurs Windows sur lesquels SafeGuard Enterprise n'est pas installé.

   Remarque : pour partager les données chiffrées stockées dans le Cloud avec les utilisateurs qui n'ont pas SafeGuard Enterprise, les utilisateurs doivent être autorisés à créer des clés locales. Retrouvez plus d'informations à la section Clés locales à la page 177.

8. Le paramètre **Dossier en texte brut** vous permet de définir un dossier qui sera exclu du chiffrement. Les données stockées dans les sous-dossiers du dossier en texte brut défini seront aussi exclues du chiffrement. SafeGuard Cloud Storage crée automatiquement des dossiers en texte brut vides dans tous les dossiers de synchronisation définis dans la **Définition Cloud Storage**.

23 Attribution utilisateur-ordinateur

SafeGuard Enterprise gère les informations concernant les utilisateurs autorisés à se connecter à une machine donnée figurant sur une liste mentionnée ci-dessous sous le nom d'AUM (Attribution utilisateur/machine).

Pour qu'un utilisateur soit inclus dans l'AUM, il doit s'être connecté une fois à un ordinateur sur lequel SafeGuard Enterprise a été installé et être inscrit dans SafeGuard Management Center comme utilisateur "complet" en termes de SafeGuard Enterprise. Un utilisateur "complet" désigne un utilisateur pour lequel un certificat a été généré après la première connexion et pour lequel un jeu de clés a été créé. Alors seulement les données de cet utilisateur peuvent être dupliquées sur d'autres ordinateurs. Après la duplication, l'utilisateur peut se connecter à cet ordinateur lors de l'authentification au démarrage SafeGuard.

Si le paramètre par défaut s'applique, le premier utilisateur à se connecter à l'ordinateur après l'installation de SafeGuard Enterprise est saisi dans l'AUM en tant que propriétaire de cet ordinateur.

Cet attribut permet à l'utilisateur s'étant authentifié lors de l'authentification au démarrage SafeGuard, d'autoriser d'autres utilisateurs à se connecter à cet ordinateur. Retrouvez plus d'informations à la section Enregistrement d'utilisateurs SafeGuard Enterprise supplémentaires à la page 89. Ils seront également ajoutés à l'AUM pour cet ordinateur.

Une liste automatique est générée et détermine quel utilisateur est autorisé à se connecter à quel ordinateur. Cette liste peut être modifiée dans SafeGuard Management Center.

23.1 Attribution utilisateur-ordinateur dans SafeGuard Management Center

Les utilisateurs peuvent être affectés à des ordinateurs spécifiques du SafeGuard Management Center. Si un utilisateur est affecté à un ordinateur dans SafeGuard Management Center (ou réciproquement) cette affectation est intégrée à l'AUM. Les données de l'utilisateur (certificat, clé etc.) sont dupliquées sur cet ordinateur et l'utilisateur peut s'y connecter. Lorsqu'un utilisateur est supprimé de l'AUM, toutes ses données utilisateur sont automatiquement supprimées de l'authentification au démarrage SafeGuard. L'utilisateur ne peut plus se connecter à l'authentification au démarrage SafeGuard avec son nom et son mot de passe.

Remarque : dans **Utilisateurs et ordinateurs**, pour visualiser l'attribution des utilisateurs et des ordinateurs, vous avez besoin au moins de droits d'accès en **Lecture seule** pour l'un des objets (utilisateur ou ordinateur) en question. Pour définir ou changer l'attribution, vous avez besoin des droits d'**Accès complet** pour les deux objets en question. L'affichage AUM montrant les utilisateurs/machines disponibles est filtré en fonction de vos droits d'accès. Dans l'affichage de la grille AUM, qui montre les utilisateurs attribués aux ordinateurs et vice-versa, les objets pour lesquels vous n'avez pas les droits d'accès requis apparaissent pour information, mais l'attribution ne peut pas être modifiée.

Lorsque vous attribuez un utilisateur à un ordinateur, vous pouvez aussi spécifier qui peut autoriser d'autres utilisateurs à se connecter à cet ordinateur.

Sous **Type**, SafeGuard Management Center indique la méthode selon laquelle l'utilisateur a été ajouté à la base de données SafeGuard Enterprise. **Adopté** signifie que l'utilisateur a été ajouté à l'AUM sur un ordinateur d'extrémité.

Remarque : si personne n'est attribué dans SafeGuard Management Center et si aucun utilisateur n'est spécifié comme propriétaire, le premier utilisateur à se connecter à l'ordinateur après l'installation de SafeGuard Enterprise est saisi en tant que propriétaire. Cet utilisateur peut ensuite autoriser d'autres utilisateurs à se connecter à cet ordinateur. Retrouvez plus d'informations à la section Enregistrement d'utilisateurs SafeGuard Enterprise supplémentaires à la page 89. Si des utilisateurs sont attribués à cet ordinateur dans SafeGuard Management Center à une date ultérieure, ils peuvent ensuite se connecter lors de l'authentification au démarrage SafeGuard. Néanmoins, ces utilisateurs doivent être des utilisateurs complets (avec un certificat et une clé existants). Le propriétaire de l'ordinateur n'a pas besoin d'attribuer des droits d'accès dans ce cas.

Les paramètres suivants permettent de spécifier qui est autorisé à ajouter des utilisateurs à l'AUM :

- **Peut devenir propriétaire** : si ce paramètre est sélectionné, l'utilisateur peut être enregistré comme le propriétaire d'un ordinateur.
- **Utilisateur propriétaire** : ce paramètre signifie que l'utilisateur est saisi dans l'AUM en tant que propriétaire. Un seul utilisateur par ordinateur peut être saisi dans l'AUM en tant que propriétaire.

  Le paramètre de stratégie **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** des **Paramètres machine spécifiques** détermine qui est autorisé à ajouter d'autres utilisateurs à l'AUM. Le paramètre **Activer l'enregistrement des utilisateurs Windows de SGN** dans les stratégies **Paramètres machine spécifiques** détermine quels utilisateurs Windows de SGN peuvent être enregistrés sur l'ordinateur d'extrémité et ajoutés à l'AUM.
- **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour**

  Personne

  Même l'utilisateur saisi comme propriétaire ne peut pas ajouter d'autres utilisateurs à l'AUM. L'option permettant à un propriétaire d'ajouter d'autres utilisateurs est désactivée.

  Propriétaire (paramètre par défaut)

  Remarque : un responsable de la sécurité peut toujours ajouter des utilisateurs dans le SafeGuard Management Center.

  Tout le monde

  Lève la restriction selon laquelle les utilisateurs ne peuvent être ajoutés que par le propriétaire.

  Remarque : pour les ordinateurs d'extrémité sur lesquels le module Protection des périphériques n'est pas installé, le paramètre **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** doit être défini sur **Tout le monde** s'il est possible d'ajouter plusieurs utilisateurs à l'Attribution utilisateur/machine avec accès à leur trousseau de clés. Autrement, les utilisateurs peuvent uniquement être ajoutés dans SafeGuard Management Center. Ce paramètre est uniquement évalué sur les ordinateurs d'extrémité administrés. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/110659.aspx.

- **Activer l'enregistrement des utilisateurs Windows de SGN**

  Si vous sélectionnez **Oui**, les utilisateurs Windows de SGN peuvent être enregistrés sur l'ordinateur d'extrémité. Un utilisateur Windows de SGN n'est pas ajouté à l'authentification au démarrage SafeGuard. En revanche, il dispose d'un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur Sophos SGN. Si vous sélectionnez ce paramètre, tous les utilisateurs, qui seraient autrement devenus des utilisateurs invités, deviennent des utilisateurs Windows de SGN. Les utilisateurs sont ajoutés à l'Attribution utilisateur/machine dès qu'ils se connectent à Windows. Les utilisateurs Windows de SGN peuvent être supprimés automatiquement de l'AUM sur les ordinateurs d'extrémité administrés et manuellement sur les ordinateurs d'extrémité non administrés. Retrouvez plus d'informations à la section Paramètres de machine spécifiques : paramètres de base à la page 141.

Exemple :

L'exemple suivant montre comment attribuer des droits de connexion dans le SafeGuard Management Center à trois utilisateurs seulement (Utilisateur_a, Utilisateur_b, Utilisateur_c) pour Ordinateur_ABC.

Premièrement : indiquez la réponse dont vous avez besoin dans SafeGuard Management Center. SafeGuard Enterprise est installé sur tous les ordinateurs d'extrémité au cours de la nuit. Le matin, les utilisateurs doivent pouvoir se connecter à leur ordinateur avec leurs codes d'accès.

1. Dans SafeGuard Management Center, attribuez Utilisateur_a, Utilisateur_b et Utilisateur_c à Ordinateur_ABC. (**Utilisateurs& ordinateurs** -> Sélectionnez Ordinateur_ABC - Attribuez l'utilisateur par Glisser-déposer). Vous avez ainsi spécifié une AUM.
2. Dans une stratégie de type **Paramètres de machine spécifiques**, définissez **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** sur **Personne**. Puisque l'Utilisateur_a, l'Utilisateur_b et l'Utilisateur_c ne sont pas autorisés à ajouter de nouveaux utilisateurs, il n'est pas nécessaire de spécifier un utilisateur comme propriétaire.
3. Attribuez la stratégie à l'ordinateur et/ou à un point de la structure du répertoire auquel elle sera active pour l'ordinateur.

Lorsque le premier utilisateur se connecte à Ordinateur_ABC, une connexion automatique est mise en œuvre pour l'authentification au démarrage SafeGuard. Les stratégies de l'ordinateur sont envoyées à l'ordinateur d'extrémité. Puisque l'Utilisateur_a est inclus dans l'AUM, il deviendra un utilisateur complet lors de sa connexion à Windows. Les stratégies de l'utilisateur, les certificats et les clés sont envoyés à l'ordinateur d'extrémité. L'authentification au démarrage SafeGuard est activée.

Remarque : l'utilisateur peut vérifier le message d'état dans l'icône de barre d'état de SafeGuard (infobulle) lorsque ce processus est terminé.

L'Utilisateur_a est à présent un utilisateur complet selon les termes de SafeGuard Enterprise et après la première connexion, il peut s'authentifier à l'authentification au démarrage SafeGuard et il est connecté automatiquement.

L'Utilisateur_a quitte à présent l'ordinateur et l'Utilisateur_b souhaite se connecter. Comme l'authentification au démarrage SafeGuard est activée, il n'y a plus de connexion automatique.

L'Utilisateur_b et l'Utilisateur_c ont deux possibilités pour accéder à cet ordinateur.

- L'Utilisateur_a désactive l'option **Connexion automatique vers Windows** dans la boîte de dialogue de connexion à l'authentification au démarrage SafeGuard et se connecte.
- L'Utilisateur_b utilise la procédure Challenge/Réponse pour se connecter à l'authentification au démarrage SafeGuard.

Dans les deux cas, la boîte de dialogue de connexion de Windows s'affiche.

L'Utilisateur_b peut saisir ses codes d'accès Windows. Les stratégies de l'utilisateur, les certificats et les clés sont envoyés à l'ordinateur d'extrémité. L'utilisateur est activé dans l'authentification au démarrage SafeGuard. L'Utilisateur_b est à présent un utilisateur complet selon les termes de SafeGuard Enterprise et après la première connexion, il peut s'authentifier lors de l'authentification au démarrage SafeGuard et sera connecté automatiquement.

Alors que la stratégie de l'ordinateur indique que personne ne peut importer d'utilisateurs sur cet ordinateur (car ces utilisateurs sont déjà dans l'AUM), l'Utilisateur_b et l'Utilisateur_c obtiennent néanmoins l'état utilisateur "complet" à la connexion Windows et sont activés dans l'authentification au démarrage SafeGuard.

Aucun autre utilisateur ne sera ajouté à l'AUM ou ne pourra s'identifier lors de l'authentification au démarrage. Tout utilisateur se connectant à Windows qui n'est pas Utilisateur_a, Utilisateur_b ou Utilisateur_c est exclu de l'AUM dans ce scénario et ne sera jamais activé dans l'authentification au démarrage SafeGuard.

Les utilisateurs peuvent toujours être ajoutés par la suite au SafeGuard Management Center. Cependant, leur jeu de clés ne sera pas disponible après la première connexion, la synchronisation n’étant pas déclenchée par la première connexion. Après une deuxième connexion, le jeu de clés sera disponible et les utilisateurs pourront accéder à leur ordinateur selon les stratégies appliquées. S’ils n’ont jamais réussi à se connecter à un ordinateur d'extrémité, il est possible de les ajouter comme indiqué ci-dessus.

23.1.1 Blocage de l'utilisateur

Si vous sélectionnez la case dans la colonne **Bloquer l'utilisateur**, l'utilisateur n'est pas autorisé à se connecter à l'ordinateur concerné. Si l'utilisateur se connecte lorsque la stratégie contenant ce paramètre est activée sur l'ordinateur, il est déconnecté.

23.1.2 Groupes

Dans SafeGuard Management Center, des groupes d'ordinateurs peuvent être attribués à un utilisateur (compte) et/ou peuvent être attribués à un ordinateur.

Pour créer un groupe : Dans **Utilisateurs et ordinateurs**, cliquez avec le bouton droit de la souris sur le nœud de l'objet approprié sur lequel vous voulez créer le groupe et sélectionnez **Nouveau**, **Créer un groupe**. Dans **Créer un groupe**, dans **Nom complet**, entrez le nom du groupe et éventuellement une description. Cliquez sur **OK**.

Exemple : Compte de service

Il est par exemple possible d'utiliser un seul compte de service pour entretenir un grand nombre d'ordinateurs. À cette fin, les ordinateurs concernés doivent se trouver dans un même groupe.

Ce groupe est ensuite attribué à un compte de service (utilisateur). Le propriétaire du compte de service peut ensuite se connecter à tous les ordinateurs de ce groupe.

En outre, le fait d'attribuer un groupe contenant différents utilisateurs permet à ces derniers de se connecter ensuite à un ordinateur spécifique en une seule étape.

23.2 Attribution de groupes d'utilisateurs et d'ordinateurs

Dans **Utilisateurs et ordinateurs**, pour visualiser l'attribution des groupes d'utilisateurs et d'ordinateurs, vous avez besoin au moins de droits d'accès en **Lecture seule** pour l'un des objets (groupe d'utilisateurs ou d'ordinateurs) en question. Pour définir ou changer l'attribution, vous avez besoin des droits d'**Accès complet** pour les deux objets en question. L'affichage AUM montrant les utilisateurs/machines disponibles est filtré en fonction de vos droits d'accès.

Remarque : vous pouvez attribuer des utilisateurs individuels à un ordinateur ou réciproquement en utilisant le même processus que pour les groupes.

1. Cliquez sur **Utilisateurs et ordinateurs**.
2. Pour attribuer un groupe d'ordinateurs à un utilisateur unique, sélectionnez ce dernier.
3. Cliquez sur l'onglet **Ordinateur** dans la zone d'action.

   Tous les ordinateurs et groupes d'ordinateurs sont affichés sous **Ordinateurs disponibles**.

4. Faites glisser les groupes sélectionnés de la liste des **Groupes disponibles** jusqu'à la zone d'activation.
5. Une boîte de dialogue s'affiche demandant si l'utilisateur doit être le propriétaire de tous les ordinateurs.

   S'il n'y a pas de propriétaire spécifique dans SafeGuard Management Center, le premier utilisateur à se connecter à cet ordinateur est automatiquement entré en tant que propriétaire. Cet utilisateur peut autoriser d'autres utilisateurs à accéder à cet ordinateur. La condition est que l'utilisateur **Peut devenir propriétaire**.

   - Si vous répondez **Oui**, le premier utilisateur à se connecter à cet ordinateur en devient le propriétaire et peut en autoriser l'accès à d'autres utilisateurs.
   - Si vous répondez **Non**, l'utilisateur ne sera pas le propriétaire de cet ordinateur.

   Il n'est généralement pas nécessaire pour le propriétaire d'un compte de service d'être en même temps le propriétaire de l'ordinateur. Ce paramètre peut être modifié après l'attribution initiale.

Tous les ordinateurs du groupe attribué sont affichés dans la zone d'action.

L'utilisateur peut se connecter à tous les ordinateurs attribués de cette manière.

Un groupe d'utilisateurs peut être attribué à un seul ordinateur en utilisant la même procédure.

24 Tokens et cartes à puce

Remarque : les tokens et les cartes à puce ne peuvent pas être configurés pour les ordinateurs d'extrémité Windows 8, Windows 8.1 et Mac.

SafeGuard Enterprise fournit une sécurité optimale en prenant en charge les tokens et cartes à puce pour authentification. Les tokens/cartes à puce peuvent stocker des certificats, signatures numériques et renseignements biométriques.

L'authentification par token est basée sur le principe d'une authentification en deux étapes : l'utilisateur possède un token (propriété), mais il ne peut l'utiliser que s'il en connaît le mot de passe (connaissance). Lorsqu'un token ou une carte à puce sont utilisés, leur présence et un code PIN suffisent à l'utilisateur pour s'authentifier.

Remarque : les cartes à puce et les tokens sont traités de la même manière dans SafeGuard Enterprise. Les termes "token" et "carte à puce" recouvrent la même notion dans le produit et le manuel.

Les tokens sont pris en charge dans SafeGuard Enterprise :

- Dans l'authentification au démarrage SafeGuard
- Au niveau du système d'exploitation
- Pour se connecter au SafeGuard Management Center

Lorsqu'un token est généré pour un utilisateur dans SafeGuard Enterprise, des informations telles que le fabricant, le type, le numéro de série, les données de connexion et les certificats sont stockées dans la base de données SafeGuard Enterprise. Les tokens sont identifiés par un numéro de série, puis reconnues dans SafeGuard Enterprise.

Les avantages sont considérables :

- Vous savez quels tokens sont en circulation et à quels utilisateurs ils ont été attribués.
- Vous connaissez la date et l'heure de leur création.
- En cas de perte d'un token, le responsable de la sécurité peut l'identifier et le bloquer. Ces mesures évitent toute utilisation frauduleuse de données.
- Toutefois, le responsable de la sécurité peut utiliser la procédure Challenge/Réponse pour autoriser temporairement la connexion sans token, par exemple si un utilisateur a oublié son code PIN.

  Remarque : cette option de récupération n'est pas prise en charge par la connexion par token cryptographique (Kerberos).

24.1 Types de token

Le terme "token" se rapporte à toutes les technologies utilisées et ne dépend pas d'une forme particulière de périphérique. Il englobe tous les périphériques pouvant stocker et transférer des données à des fins d'identification et d'authentification (cartes à puce ou tokens USB).

SafeGuard Enterprise prend en charge les types suivants de tokens/cartes à puce pour l'authentification :

- **Non cryptographique**

  L'authentification au démarrage SafeGuard et Windows est basée sur les codes d'accès de l'utilisateur (ID utilisateur/mot de passe) stockés sur le token.

- **Cryptographique - Kerberos**

  L'authentification au démarrage SafeGuard et Windows est basée sur les certificats stockés sur le token.

  Remarque : les tokens cryptographiques ne peuvent pas être utilisés pour les ordinateurs d'extrémité non administrés.

24.1.1 Tokens cryptographiques - Kerberos

Avec les tokens cryptographiques, l'utilisateur est identifié à l'authentification au démarrage SafeGuard par le certificat stocké sur le token. Pour se connecter au système, il suffit à l'utilisateur de saisir le code PIN du token.

Remarque : les tokens cryptographiques ne peuvent pas être utilisés pour les ordinateurs d'extrémité non administrés.

Vous devez fournir des tokens aux utilisateurs. Retrouvez plus d'informations à la section Configuration de l'utilisation d'un token à la page 202.

Conditions requises de base pour les certificats :

- Algorithme : RSA
- Longueur de la clé : minimum 1024
- Utilisation de la clé : *chiffrement de données* ou *chiffrement de clés*. Une stratégie peut remplacer cette utilisation.
- Auto-signé : Non. Une stratégie peut remplacer cette utilisation.

Remarque : en cas de problèmes de connexion avec un token Kerberos, il n'est pas possible d'utiliser la procédure Challenge/Réponse ou Local Self Help pour la récupération de la connexion. Seule la procédure Challenge/Réponse utilisant les clients virtuels est prise en charge. Elle permet aux utilisateurs de récupérer l'accès aux volumes chiffrés sur leurs ordinateurs d'extrémité.

24.2 Composants

Pour utiliser les tokens/cartes à puce avec SafeGuard Enterprise, les composants suivants sont requis :

- Token/carte à puce
- Lecteur de token/carte à puce
- Pilote de token/carte à puce

- Middleware de token/carte à puce (module PKCS#11)

Tokens USB

De même que les cartes à puce, les tokens USB comportent une carte à puce et un lecteur de cartes à puce dans un même boîtier. L'utilisation des tokens USB nécessite la présence d'un port USB.

24.2.1 Lecteurs et pilotes de token/carte à puce

- **Windows**

  Dans le système d'exploitation Windows, les lecteurs de cartes compatibles PC/SC sont pris en charge. L'interface PC/SC régit la communication entre l'ordinateur et la carte à puce. La majorité de ces lecteurs de cartes sont déjà intégrés dans l'installation de Windows. Pour être prises en charge par SafeGuard Enterprise, les cartes à puce requièrent des pilotes compatibles PKCS#11.

- **Authentification au démarrage SafeGuard**

  Avec l'authentification au démarrage SafeGuard, c'est l'interface PC/SC qui régit la communication entre le PC et la carte à puce. Les pilotes de cartes à puce pris en charge sont fixés, de sorte que les utilisateurs ne peuvent pas en ajouter. Les pilotes de cartes à puce appropriés doivent être activés au moyen d'une stratégie dans SafeGuard Enterprise.

  L'interface des lecteurs de cartes à puce est standardisée et un grand nombre de ces lecteurs possèdent une interface USB ou une interface ExpressCard/54 et mettent en œuvre la norme CCID. Dans SafeGuard Enterprise, il s'agit d'une condition préalable à la prise en charge avec l'authentification au démarrage SafeGuard. De plus, du côté du pilote, le module PKCS#11 doit être pris en charge.

24.2.2 Tokens et cartes à puce pris en charge par l'authentification au démarrage SafeGuard

SafeGuard Enterprise prend en charge une large variété de cartes à puce et de lecteurs de carte à puce, de tokens USB et de leurs pilotes respectifs ainsi que de middlewares grâce à l'authentification au démarrage SafeGuard. Avec SafeGuard Enterprise, les tokens/cartes à puce compatibles avec les opérations 2048 bits RSA sont pris en charge.

La prise en charge des tokens et cartes à puce faisant l'objet d'améliorations d'une version à l'autre, les tokens et cartes à puce de la version actuelle de SafeGuard Enterprise sont répertoriés dans les notes de publication.

24.2.3 Middlewares pris en charge

Les middlewares de la liste ci-dessous sont pris en charge par le module PKCS#11 correspondant. PKCS#11 est une interface standard servant à connecter des tokens cryptographiques/cartes à puce à différents logiciels. Elle est utilisée ici pour la communication entre le token cryptographique/carte à puce, le lecteur de carte à puce et SafeGuard Enterprise. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/112781.aspx.

Fabricant	Middleware
ActivIdentity	ActivClient, ActivClient (PIV)
Aladdin	eToken PKI Client
A-Trust	a.sign Client
Charismatics	Smart Security Interface
Gemalto	Gemalto Access Client, Gemalto Classic Client, Gemalto .NET Card
Solution informatique GmbH	IT Solution trustWare CSP+
Nexus	Nexus Personal
RSA	RSA Authentication Client 2.x, RSA Smart Card Middleware 3.x
Sertifitseerimiskeskus AS	Estonian ID Card
Siemens	CardOS API
T-Systems	NetKey 3.0
Unizeto	proCertum

Licences

Sachez que l'utilisation des middlewares respectifs pour le système d'exploitation standard requiert un accord de licence avec le fabricant correspondant. Retrouvez plus d'informations sur les licences dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/116585.aspx.

Pour les licences Siemens, contactez

Atos IT Solutions and Services GmbH

Otto-Hahn-Ring 6

81739 Muenchen

Allemagne

Le middleware est défini dans une stratégie SafeGuard Enterprise de type **Paramètres de machine spécifiques** sous **Paramètres PKCS#11 personnalisés** dans le champ **Module PKCS#11 pour Windows** ou **Module PKCS#11 pour l'authentification au démarrage**. Le package de configuration correspondant doit également être installé sur l'ordinateur sur lequel fonctionne SafeGuard Management Center.

24.3 Configuration de l'utilisation d'un token

Procédez aux étapes suivantes si vous voulez fournir des tokens aux utilisateurs suivants à des fins d'authentification :

- Utilisateurs d'ordinateurs d'extrémité administrés
- Responsables de la sécurité de SafeGuard Management Center

1. Initialiser les tokens vides.

   Retrouvez plus d'informations à la section Initialisation d'un token à la page 203.

2. Installer le middleware.

   Retrouvez plus d'informations à la section Installation du middleware à la page 203.

3. Activer le middleware.

   Retrouvez plus d'informations à la section Activation du middleware à la page 203.

4. Générer des tokens pour les utilisateurs et les responsables de la sécurité.

   Retrouvez plus d'informations à la section Génération d'un token à la page 204.

5. Configurer le mode de connexion.

   Retrouvez plus d'informations à la section Configuration du mode de connexion à la page 206.

6. Configurer d'autres paramètres de token comme par exemple, les règles de syntaxe des codes PIN.

   Retrouvez plus d'informations à la section Gestion des codes PIN à la page 211 et à la section Gestion des tokens et des cartes à puce à la page 212.

7. Attribuer des certificats et des clés aux tokens/utilisateurs.

   Retrouvez plus d'informations à la section Attribution de certificats à la page 207.

Vous pouvez également utiliser des tokens dont les données proviennent d'une application différente pour l'authentification à condition qu'ils disposent de suffisamment d'espace de stockage pour les certificats et les informations de connexion.

Pour une administration simplifiée des tokens, SafeGuard Enterprise propose les fonctions suivantes :

- Affichage et filtrage des informations du token
- Initialisation, modification, réinitialisation et blocage des codes PIN
- Lecture et suppression des données du token
- Blocage des tokens

Remarque : pour générer et gérer des tokens ou modifier des données sur les tokens générés, vous avez besoin des droits d'**Accès complet** pour les utilisateurs concernés. La vue **Tokens générés** n'affiche que les tokens des utilisateurs pour qui vous avez des droits en **Lecture seule** ou d'**Accès complet**.

24.4 Préparation à l'utilisation d'un token

Pour préparer la prise en charge d'un token ou d'une carte à puce dans SafeGuard Enterprise, veuillez :

- Initialiser les tokens vides.
- Installer le middleware.
- Activer le middleware.

24.4.1 Initialisation d'un token

Avant qu'un token "vide" non formaté puisse être généré, il doit être préparé pour l'utilisation, c'est-à-dire initialisé, conformément aux instructions fournies par son fabricant. Lorsqu'il est initialisé, des informations de base, par exemple le code PIN standard, sont écrites dessus. Cette opération s'effectue avec le logiciel d'initialisation du fabricant de tokens.

Retrouvez plus d'informations chez le fabricant de tokens concerné.

24.4.2 Installation du middleware

Veuillez installer le middleware qui convient, à la fois sur l'ordinateur sur lequel SafeGuard Management Center est installé et sur l'ordinateur d'extrémité approprié, si vous ne l'avez pas déjà fait. Retrouvez plus d'informations sur les middlewares pris en charge à la section Middlewares pris en charge à la page 200.

Redémarrez les ordinateurs sur lesquels vous avez installé le nouveau middleware.

Remarque : si vous installez le middleware **Gemalto .NET Card** ou **Nexus Personal**, vous allez également devoir ajouter leur chemin d'installation à la variable d'environnement PATH des **Propriétés système** de votre ordinateur.

- Le chemin d'installation par défaut pour **Gemalto .NET Card** : `C:\Program Files\Gemalto\PKCS11 for .NET V2 smart cards`
- Le chemin d'installation par défaut pour **Nexus Personal** : `C:\Program Files\Personal\bin`

24.4.3 Activation du middleware

Veuillez attribuer le middleware approprié sous la forme du module PKCS#11 en définissant une stratégie dans SafeGuard Management Center. Vous devez le faire à la fois sur l'ordinateur sur lequel SafeGuard Management Center est exécuté et sur l'ordinateur d'extrémité. C'est la condition nécessaire pour que SafeGuard Enterprise communique avec le token. Vous pouvez définir le paramètre du module PKCS#11 en utilisant une stratégie, de la façon suivante.

Condition préalable : le middleware est installé sur l'ordinateur concerné et le token a été initialisé. Le package de configuration du client SafeGuard Enterprise doit également être installé sur l'ordinateur PC sur lequel SafeGuard Management Center est exécuté.

1. Dans SafeGuard Management Center, cliquez sur **Stratégies**.

2. Créez une nouvelle stratégie du type **Paramètres de machine spécifiques** ou sélectionnez une stratégie existante de ce type.
3. Dans la zone de travail côté droit, sélectionnez le middleware approprié sous **Paramètres de prise en charge du token** > **Nom du module**. Enregistrez les paramètres.
4. Attribuez la stratégie.

À présent, SafeGuard Enterprise peut communiquer avec le token.

24.5 Génération d'un token

Lorsqu'un token est généré dans SafeGuard Enterprise, les données qui sont utilisées pour l'authentification sont écrites sur ce token. Ces données sont constituées de codes d'accès et de certificats.

Dans SafeGuard Enterprise, des tokens peuvent être générés pour les rôles d'utilisateurs suivants :

- Tokens pour les utilisateurs des ordinateurs d'extrémité administrés
- Tokens pour les responsables de la sécurité

L'utilisateur et les responsables de la sécurité peuvent accéder au token. L'utilisateur est celui qui doit utiliser le token. L'utilisateur n'a accès qu'aux objets et aux clés privés. Le responsable de la sécurité peut uniquement accéder aux objets publics, mais il peut réinitialiser le code PIN de l'utilisateur.

24.5.1 Génération d'un token ou d'une carte à puce pour un utilisateur

Conditions préalables :

- le token doit être initialisé et le module PKCS#11 approprié doit être activé.
- Le package de configuration du client SafeGuard Enterprise doit également être installé sur l'ordinateur PC sur lequel SafeGuard Management Center est exécuté.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Connectez le token à l'interface USB. SafeGuard Enterprise lit le token.
3. Sélectionnez l'utilisateur pour lequel un token doit être généré, et ouvrez l'onglet **Données de token** dans la zone de travail du côté droit.
4. Dans l'onglet **Données de token**, procédez comme suit :

   a) Sélectionnez l'**ID utilisateur** et le **Domaine** de l'utilisateur concerné et saisissez votre **Mot de passe** Windows.

   b) Cliquez sur **Générer un token**.

   La boîte de dialogue **Génération d'un token** s'affiche.

5. Sélectionnez le connecteur adapté au token dans la liste déroulante **Connecteurs disponibles**.

6. Générez un nouveau **Code PIN utilisateur** et répétez la saisie.
7. Sous **PIN SO**, saisissez le code PUK standard fourni par le fabricant ou le code PIN généré lorsque le token a été initialisé.

   Remarque : si vous remplissez uniquement le champ **Code PIN utilisateur** (**obligatoire**), le code PIN de l'utilisateur doit correspondre à celui qui a été généré lors de l'initialisation du token. Il est alors inutile de répéter le code PIN de l'utilisateur ou de saisir un code PIN du SO.

8. Cliquez sur **Générer un token maintenant**.

Le token est généré, les informations de connexion écrites sur le token et les informations de token enregistrées dans la base de données SafeGuard Enterprise. Vous pouvez afficher les données de la zone **Token** dans l'onglet **Informations sur le token**.

24.5.2 Génération d'un token ou d'une carte à puce pour un responsable de la sécurité

Lorsque SafeGuard Enterprise est installé pour la première fois, le premier responsable de la sécurité peut générer pour lui-même un token et indiquer le mode de connexion (consultez le *Guide d'installation SafeGuard Enterprise*). Pour tous les autres responsables de la sécurité, les tokens sont générés dans SafeGuard Management Center.

Condition préalable :

- le token doit être initialisé et le module PKCS#11 approprié doit être activé.
- Vous devez disposer des droits nécessaires pour effectuer des sélections pour le responsable de la sécurité.

1. Dans SafeGuard Management Center, cliquez sur **Responsables de la sécurité**.
2. Connectez le token à l'interface USB. SafeGuard Enterprise lit le token.
3. Dans la fenêtre de navigation de gauche, cochez **Responsable de la sécurité** et sélectionnez **Nouveau** > **Nouveau responsable de la sécurité** dans le menu contextuel.

   La boîte de dialogue **Nouveau responsable de la sécurité** s'affiche.

4. Dans le champ **Connexion au token**, spécifiez le type de connexion pour le responsable de la sécurité :
   - Pour permettre au responsable de la sécurité de s'authentifier avec ou sans token, sélectionnez **Facultatif**.
   - Pour rendre obligatoire la connexion sur la carte à puce pour le responsable de la sécurité, sélectionnez **Obligatoire**.

     Avec ce paramètre, la clé privée reste sur le token. Le token doit toujours être connecté, sinon, le système doit être réinitialisé.

5. Veuillez, ensuite, indiquer le certificat du responsable de la sécurité.
   - Pour créer un nouveau certificat, cliquez sur le bouton **Créer** près de la liste déroulante **Certificat**.

     Saisissez un mot de passe pour le certificat deux fois et cliquez sur **OK** pour le confirmer.

     Indiquez l'emplacement d'enregistrement du certificat.
   - Pour importer les certificats, cliquez sur le bouton **Importer** près de la liste déroulante **Certificat** et ouvrez le fichier de certificat correspondant.

     La recherche s'effectue d'abord dans un fichier de certificat, puis sur le token. Les certificats peuvent rester dans l'emplacement de stockage quel qu'il soit.
6. Sous **Rôles**, activez les rôles devant être attribués au responsable de la sécurité.
7. Confirmez les saisies en cliquant sur **OK**.

Le responsable de la sécurité est créé, le token est généré, les informations de connexion sont écrites sur le token (en fonction du paramètre) et les informations du token sont enregistrées dans la base de données SafeGuard Enterprise. Vous pouvez afficher les données de la zone **Token** dans l'onglet **Informations sur le token**.

24.6 Configuration du mode de connexion

Il existe deux méthodes de connexion à l'aide d'un token. Il est possible de combiner les deux méthodes de connexion.

- Connexion avec identifiant utilisateur/mot de passe
- Connexion avec token

  Lorsque vous vous connectez avec un token ou une carte à puce, vous pouvez sélectionner la méthode non cryptographique ou la méthode Kerberos (cryptographique).

En tant que responsable de la sécurité, vous spécifiez le mode de connexion à utiliser dans une stratégie du type **Authentification**.

Si vous sélectionnez l'option de connexion par token **Kerberos** :

- Vous allez devoir émettre un certificat dans une infrastructure de clé publique (PKI) et la stocker sur le token. Ce certificat est importé sous forme de certificat utilisateur dans la base de données SafeGuard Enterprise. Si un certificat généré automatiquement existe déjà dans une base de données, il est remplacé par le certificat importé.

24.6.1 Activation de la connexion automatique à l'authentification au démarrage SafeGuard avec des codes PIN de token par défaut

Un code PIN de token par défaut distribué par la stratégie permet la connexion automatique de l'utilisateur à l'authentification au démarrage SafeGuard. Ceci permet d'éviter la génération de chaque token séparément et permet aux utilisateurs de se connecter automatiquement lors de l'authentification au démarrage SafeGuard sans intervention de l'utilisateur.

Lorsqu'un token est utilisée lors de la connexion et qu'un code PIN par défaut est attribué à l'ordinateur, l'utilisateur est connecté automatiquement à l'authentification au démarrage SafeGuard sans qu'il ait besoin de saisir un code PIN.

En tant que responsable de la sécurité, vous pouvez définir le code PIN spécifique dans une stratégie du type **Authentification** et l'attribuer à différents ordinateurs ou groupes d'ordinateurs, par exemple à tous les ordinateurs d'un même lieu.

Pour activer la connexion automatique avec un code PIN de token par défaut, procédez comme suit :

1. Dans SafeGuard Management Center, cliquez sur **Stratégies**.
2. Sélectionnez une stratégie du type **Authentification**.
3. Sous **Options de connexion**, dans **Mode de connexion**, sélectionnez **Token**.
4. Dans **Code PIN utilisé pour la connexion automatique avec token**, spécifiez le code PIN par défaut à utiliser pour la connexion automatique. Dans ce cas, il n'est pas nécessaire de suivre les règles relatives au code PIN.

   Remarque : ce paramètre n'est disponible que si vous sélectionnez **Carte à puce** comme **Mode de connexion** possible.

5. Dans **Connexion automatique vers Windows**, définissez **Désactiver la connexion automatique vers Windows**. Si vous ne sélectionnez pas cette option lorsqu'un code PIN par défaut est spécifié, vous ne pourrez pas enregistrer la stratégie.

   Si vous souhaitez activer l'option **Connexion automatique vers Windows**, vous pouvez créer ultérieurement une autre stratégie du type **Authentification** dans laquelle cette option est activée, et l'attribuer au même groupe d'ordinateurs afin que les deux stratégies soient actives dans le RSOP.
6. Vous pouvez également spécifier d'autres paramètres de token.
7. Enregistrez vos paramètres et attribuez la stratégie aux ordinateurs ou groupes d'ordinateurs concernés.

Windows démarre si la connexion automatique sur l'ordinateur d'extrémité réussit.

En cas d'échec de la connexion automatique sur l'ordinateur d'extrémité, l'utilisateur est invité à saisir le code PIN de token lors de l'authentification au démarrage SafeGuard.

24.7 Attribution de certificats

Les informations de connexion, mais également les certificats peuvent être écrits sur un token. Seule la partie privée du certificat (fichier .p12) peut être enregistrée sur le token. En revanche, les utilisateurs peuvent alors seulement se connecter avec le token. Nous vous recommandons d'utiliser des certificats PKI.

Vous pouvez attribuer les données d'authentification à différents types de tokens de la manière suivante :

- En générant des certificats directement sur le token
- En attribuant des données qui sont déjà sur le token

- En important des certificats d'un fichier.

Remarque : les certificats de l'AC ne peuvent pas provenir d'un token et être stockés dans la base de données ou dans le magasin de certificats. Si vous utilisez des certificats de l'AC, ces derniers doivent être disponibles sous forme de fichiers et pas seulement sur un token. Ceci s'applique également aux CRL (liste de révocation des certificats). De surcroît, les certificats de l'AC doivent correspondre à la liste de révocation de certificats pour que les utilisateurs puissent se connecter aux ordinateurs concernés. Vérifiez que l'AC et que la liste de révocation de certificats correspondante sont correctes. SafeGuard Enterprise n'effectue pas cette vérification. SafeGuard Enterprise ne peut ensuite communiquer avec les certificats ayant expiré que si les clés nouvelles et anciennes sont présentes sur la même carte.

24.7.1 Génération de certificats à partir de tokens

Pour générer des certificats à partir de tokens, vous avez besoin des droits d'**Accès complet** pour l'utilisateur concerné.

Vous pouvez générer de nouveaux certificats directement à partir du token si, par exemple, aucune structure de certificat n'est présente.

Remarque : si seule la partie privée du certificat est écrite sur le token, l'utilisateur peut seulement accéder à sa clé privée avec ce token. La clé privée ne se trouve alors que sur le token. En cas de perte du token, la clé privée devient inaccessible.

Condition préalable : le token a été généré.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Connectez le token dans l'interface USB.

   SafeGuard Enterprise lit le token.

3. Cochez l'utilisateur pour lequel un certificat doit être généré, et ouvrez l'onglet **Certificat** dans la zone de travail du côté droit.
4. Cliquez sur **Générer et attribuer un certificat par token**. Notez que la longueur de la clé doit correspondre à la taille du token.
5. Sélectionnez le connecteur et saisissez le code PIN du token.
6. Cliquez sur **Créer**.

Le token génère le certificat et l'attribue à l'utilisateur.

24.7.2 Attribution de certificats de token à un utilisateur

Conditions préalables :

- le token a été généré.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

Pour attribuer un certificat disponible sur un token à un utilisateur :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.

2. Connectez le token dans l'interface USB.

   SafeGuard Enterprise lit le token.

3. Sélectionnez l'utilisateur à qui vous voulez attribuer un certificat et ouvrez l'onglet **Certificat** dans la zone de travail à droite.
4. Cliquez sur l'icône **Attribuer un certificat à partir d'un token** de la barre d'outils du SafeGuard Management Center.
5. Sélectionnez le certificat concerné dans la liste et saisissez le code PIN du token.
6. Cliquez sur **OK**.

Le certificat est attribué à un l'utilisateur. Un seul certificat peut être affecté par utilisateur.

24.7.3 Modification du certificat de l'utilisateur

Vous pouvez modifier ou renouveler les certificats requis pour la connexion en attribuant un nouveau certificat dans SafeGuard Management Center. Le certificat est attribué sous la forme d'un certificat de veille en compagnie de celui existant. En se connectant avec le nouveau certificat, l'utilisateur change le certificat sur l'ordinateur d'extrémité.

Remarque : si les utilisateurs ont perdu leurs tokens ou si ceux-ci ont été compromis. Ne les échangez pas en attribuant de nouveaux certificats comme cela est décrit ici. Sinon, vous pourriez rencontrer des problèmes. Par exemple, l'ancien certificat de token peut être encore valide pour la connexion Windows. Tant que l'ancien certificat est encore valide, la connexion à Windows est toujours possible et l'ordinateur peut être déverrouillé. Au lieu de cela, bloquez le token pour empêcher la connexion.

Les certificats de veille peuvent être utilisés dans les cas suivants :

- Modification des certificats générés par token (cryptographique).
- Passage de certificats générés automatiquement à des certificats générés par token.
- Passage d'une authentification par nom utilisateur/mot de passe à une authentification par token cryptographique (Kerberos).

Conditions préalables :

- Le nouveau token a été généré.
- Seul un certificat est attribué à l'utilisateur.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

Pour changer le certificat d'un utilisateur pour la connexion par token :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Connectez le token dans l'interface USB.

   SafeGuard Enterprise lit le token.

3. Sélectionnez l'utilisateur dont vous voulez changer le certificat et ouvrez l'onglet **Certificat** dans la zone de travail à droite.
4. Dans la barre d'outils, cliquez sur l'icône appropriée pour l'action que vous voulez exécuter.

5. Sélectionnez le certificat concerné et saisissez le code PIN du token.
6. Cliquez sur **OK**.
7. Fournissez le nouveau token à l'utilisateur.

Le certificat est attribué à l'utilisateur sous la forme d'un certificat de veille. Ceci est indiqué par une coche dans la colonne **Veille** de l'onglet **Certificats** de l'utilisateur.

Après la synchronisation entre l'ordinateur d'extrémité et le serveur SafeGuard Enterprise, la boîte de dialogue d'état de l'ordinateur d'extrémité indique que ce dernier est **Prêt pour la modification du certificat**.

L'utilisateur doit maintenant lancer une modification du certificat sur l'ordinateur d'extrémité. Retrouvez plus d'informations dans le *Manuel d'utilisation de SafeGuard Enterprise*.

Une fois que l'utilisateur a changé le certificat sur l'ordinateur d'extrémité, le certificat est également renouvelé sur le serveur SafeGuard Enterprise lors de la synchronisation suivante. Cela supprime l'ancien token de l'onglet **Certificats** de l'utilisateur dans SafeGuard Management Center. Le nouveau token devient le token standard pour l'utilisateur.

Remarque : dans SafeGuard Management Center, les deux certificats peuvent être supprimés séparément. Si un seul certificat de veille est disponible, le certificat suivant est attribué sous la forme d'un certificat de veille.

24.7.4 Importation d'un certificat à partir d'un fichier du token

Condition préalable : le token a été généré.

Vous devez sélectionner cette procédure pour un token avec la prise en charge Kerberos. Le certificat doit être reconnu par SafeGuard Enterprise et ajouté au token. S'il existe déjà un certificat généré automatiquement, le certificat importé le remplacera.

Pour ajouter la partie privée du certificat (fichier .p12) sur le token à partir d'une fichier :

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. Connectez le token dans l'interface USB.

   SafeGuard Enterprise lit le token.

3. Marquez le token auquel vous voulez ajouter la partie privée du certificat et, dans la zone de travail à droite, ouvrez l'onglet **Informations de connexion et certificats**.
4. Cliquez sur l'icône **P12 à token** dans la barre d'outils du SafeGuard Management Center.
5. Sélectionnez le fichier de certificat concerné.
6. Saisissez le code PIN du token et le mot de passe du fichier .p12 et confirmez en cliquant sur **OK**.

La partie privée du certificat est ajoutée au token. À présent, vous devez l'attribuer à un utilisateur. Retrouvez plus d'informations à la section Attribution de certificats de token à un utilisateur à la page 208. Les utilisateurs peuvent alors seulement se connecter avec ce token.

24.8 Gestion des codes PIN

En tant que responsable de la sécurité, vous pouvez changer le code PIN de l'utilisateur et celui du responsable de la sécurité et aussi forcer le changement du code PIN de l'utilisateur. Ceci est généralement nécessaire lors de la génération d'un token. Vous pouvez également initialiser des codes PIN, c'est-à-dire les générer comme de nouveaux codes PIN, et les bloquer.

Remarque : pour initialiser, changer et bloquer les codes PIN, vous avez besoin des droits d'**Accès complet** pour les utilisateurs correspondants.

Vous pouvez utiliser des stratégies pour spécifier d'autres options de code PIN pour l'ordinateur d'extrémité.

Remarque : lorsque vous changez un code PIN, certains fabricants de tokens spécifient leurs propres règles de code PIN qui peuvent contredire celles de SafeGuard Enterprise. C'est la raison pour laquelle il se peut qu'il ne soit pas possible de changer un code PIN comme vous le souhaitez, même s'il respecte les règles des codes PIN de SafeGuard Enterprise. Vous devez toujours consulter les règles des codes PIN du fabricant de tokens. Elles peuvent être affichées dans la zone **Token** sous **Informations sur le token** dans SafeGuard Management Center.

Les codes PIN sont gérés dans SafeGuard Management Center sous **Tokens**. Le token est connecté et coché dans la fenêtre de navigation de gauche.

24.8.1 Initialisation du code PIN utilisateur

Conditions préalables :

- Le code PIN du SO doit être connu.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

1. Dans la barre d'outils du SafeGuard Management Center, cliquez sur **Initialiser le PIN utilisateur**.
2. Saisissez le code PIN du SO.
3. Saisissez le nouveau code PIN de l'utilisateur, répétez la saisie et confirmez en cliquant sur **OK**.

Le code PIN de l'utilisateur est initialisé.

24.8.2 Changement du code PIN d'un responsable de la sécurité

Condition préalable : le code PIN du responsable de la sécurité précédent doit être connu.

1. Dans la barre d'outils du SafeGuard Management Center, cliquez sur l'icône **Changer le code PIN SO**.
2. Saisissez l'ancien code PIN du SO.
3. Saisissez le nouveau code PIN du SO, répétez la saisie et cliquez sur **OK**.

Le code PIN du SO a été modifié.

24.8.3 Changement d'un code PIN utilisateur

Condition préalable :

- Le code PIN de l'utilisateur doit être connu.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

1. Dans la barre d'outils du SafeGuard Management Center, cliquez sur l'icône **Changer le code PIN de l'utilisateur**.
2. Saisissez l'ancien et le nouveau code PIN de l'utilisateur, répétez la saisie du nouveau et confirmez en cliquant sur **OK**.

Le code PIN de l'utilisateur est changé. Si vous avez changé le code PIN d'un autre utilisateur, informez-le de cette modification.

24.8.4 Changement forcé du code PIN

Pour forcer le changement d'un code PIN, vous avez besoin des droits d'**Accès complet** pour l'utilisateur concerné.

1. Dans la barre d'outils du SafeGuard Management Center, cliquez sur **Forcer le changement du code PIN**.

Lors de la prochaine connexion de l'utilisateur avec le token, il doit changer son code PIN.

24.8.5 Historique des codes PIN

L'historique des codes PIN peut être supprimé. Pour cela, cliquez sur l'icône **Supprimer l'historique de PIN** de la barre d'outils du SafeGuard Management Center.

24.9 Gestion des tokens et des cartes à puce

Dans la zone **Tokens** du SafeGuard Management Center, le responsable de la sécurité peut :

- Avoir un aperçu des tokens et des certificats qui ont été générés.
- Filtrer des aperçus.
- Bloquer les tokens pour authentification.
- Lire ou supprimer les données sur un token.

24.9.1 Affichage des informations du token/carte à puce

En tant que responsable de la sécurité, vous pouvez afficher des informations sur tous les tokens ou sur certains tokens ayant été générés. Vous pouvez aussi filtrer les aperçus.

Condition préalable : le token doit être connecté.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.

2. Pour afficher des informations sur un token individuel, sélectionnez le token correspondant dans la zone de navigation sous **Connecteurs de tokens**.

   Le fabricant, le type, le numéro de série, les données matérielles et les règles des codes PIN sont affichés sous **Informations sur le token**. Vous pouvez également voir à quel utilisateur le token est attribué.

   Remarque : sous **Connecteurs de tokens**, les tokens générés apparaissent quels que soient vos droits d'accès aux utilisateurs concernés. Vous pouvez ainsi voir si le token est en cours d'utilisation ou non. Si vous n'avez pas de droits d'accès en **Lecture seule** à l'utilisateur attribué, toutes les données sur les tokens dans les onglets **Informations sur le token** et **Informations d'identification et certificats** sont grisées et vous ne pouvez pas gérer ce token.

3. Pour afficher un aperçu des tokens, sélectionnez **Tokens générés**. Vous pouvez afficher toutes les cartes à puce ayant été générées ou filtrer l'aperçu par utilisateur.

   Le numéro de série du token, les utilisateurs attribués et la date de génération sont affichés. Vous pouvez également voir si le token est bloqué.

   Remarque : la vue **Tokens générés** n'affiche que les tokens des utilisateurs pour qui vous avez des droits en **Lecture seule** ou d'**Accès complet**.

24.9.2 Blocage d'un token ou d'une carte à puce

Si vous êtes responsable de la sécurité, vous pouvez bloquer des tokens. C'est utile, par exemple, si un token a été perdu.

Pour bloquer un token, vous avez besoin des droits d'**Accès complet** pour l'utilisateur concerné.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. Dans la zone de navigation de gauche, sélectionnez **Tokens générés** à gauche de la zone de navigation.
3. Sélectionnez le token à bloquer et cliquez sur l'icône **Bloquer le token** de la barre d'outils du SafeGuard Management Center.

Le token est bloqué pour l'authentification et l'utilisateur attribué ne peut plus l'utiliser pour se connecter. Le token ne peut être débloqué qu'en utilisant le code PIN du responsable de la sécurité.

24.9.3 Suppression des informations du token/carte à puce

En tant que responsable de la sécurité, vous pouvez supprimer les informations écrites sur le token par SafeGuard Enterprise.

Condition préalable :

- le token doit être connecté.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.

2. Dans la zone de navigation de gauche, sélectionnez la carte à puce concernée sous **Cartes à puce générées**.
3. Dans la barre d'outils du SafeGuard Management Center, cliquez sur **Effacer la clé**.
4. Saisissez le code PIN du responsable de la sécurité qui a été attribué au token et confirmez en cliquant sur **OK**.

Toutes les données gérées par SafeGuard Enterprise sont supprimées. Les certificats restent sur le token.

Le code PIN de l'utilisateur est réinitialisé à 1234.

les tokens effacés sont ainsi automatiquement supprimées de la liste des tokens générés.

24.9.4 Lecture des informations de token/carte à puce

En tant que responsable de la sécurité, vous pouvez lire les données sur le token à l'aide du code PIN utilisateur.

Condition préalable :

- Le token doit être connecté. Le responsable de la sécurité doit connaître le code PIN. Ou il doit être initialisé. Retrouvez plus d'informations à la section Initialisation du code PIN utilisateur à la page 211.
- Vous avez besoin des droits en **Lecture seule** ou d'**Accès complet** pour l'utilisateur correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. À gauche de la zone de navigation, sélectionnez le token approprié sous **Connecteurs de tokens** et sélectionnez l'onglet **Codes d'accès & certificats**.
3. Cliquez sur l'icône **Obtenir les codes d'accès utilisateur** et saisissez le code PIN utilisateur du token.

Les données du token s'affichent.

25 Éveil par appel réseau sécurisé (WOL)

Dans SafeGuard Management Center, vous pouvez définir des paramètres de stratégie pour l'**Éveil par appel réseau sécurisé (WOL)** afin de préparer les ordinateurs d'extrémité à des déploiements logiciels. Si une stratégie correspondante s'applique aux ordinateurs d'extrémité, les paramètres nécessaires (par exemple, la désactivation de l'authentification au démarrage SafeGuard et un intervalle d'éveil par appel réseau) sont transférés directement sur les ordinateurs d'extrémité lorsque les paramètres sont analysés.

L'équipe de déploiement peut concevoir un script de programmation en utilisant les commandes fournies pour garantir la protection maximale de l'ordinateur d'extrémité malgré la désactivation de l'authentification au démarrage SafeGuard.

Remarque : la désactivation de l'authentification au démarrage SafeGuard (même pour un nombre limité de processus d'initialisation) réduit le niveau de sécurité de votre système.

Définissez les paramètres de l'**Éveil par appel réseau (WOL)** dans une stratégie du type **Paramètres de machine spécifiques**.

25.1 Exemple d'éveil par appel réseau sécurisé

L'équipe de déploiement des logiciels informe le responsable de la sécurité SafeGuard Enterprise d'un déploiement de logiciels prévu pour le 25 septembre 2013 entre 03:00 et 06:00 heures du matin. Deux réinitialisations sont requises. L'agent local en charge du déploiement des logiciels doit être en mesure de se connecter à Windows.

Dans SafeGuard Management Center, le responsable de la sécurité crée une stratégie du type **Paramètres de machine spécifiques** avec les paramètres suivants et l'attribue aux ordinateurs d'extrémité souhaités.

Paramètre de stratégie	Valeur
Nombre de connexions automatiques (0 = pas de WOL) :	5
Autoriser la connexion à Windows pendant le WOL	Oui
Début de la tranche horaire pour le lancement du WOL externe	24 sept. 2013, 12:00
Fin de la tranche horaire pour le lancement du WOL externe	25 sept. 2013, 06:00

Retrouvez plus d'informations sur les paramètres individuels à la section Paramètres de machine spécifiques : paramètres de base à la page 141.

Étant donné que le nombre de connexions automatiques est défini sur 5, l'ordinateur d'extrémité démarre 5 fois sans identification à l'authentification au démarrage SafeGuard.

Remarque : pour le mode Éveil par appel réseau, nous vous conseillons d'autoriser **trois redémarrages de plus que nécessaire** pour faire face aux problèmes imprévus.

Le responsable de la sécurité définit l'intervalle sur 12 heures ou midi le jour précédant le déploiement de logiciels. Ainsi, le script de planification SGMCMDIntn.exe démarre à l'heure et l'éveil par appel réseau ne se lance qu'à partir du 25 septembre à 3 heures du matin.

L'équipe de déploiement des logiciels crée deux commandes pour le script de programmation :

- Démarrage 24 sept. 2013, 12:15, SGMCMDIntn.exe -WOLstart
- Démarrage 26 sept. 2013, 09:00 SGMCMDIntn.exe -WOLstop

Le script de déploiement des logiciels est daté du 25.09.2013, 03:00. L'éveil par appel réseau peut être à nouveau explicitement désactivé à la fin du script en utilisant SGMCMDIntn.exe -WOLstop.

Tous les ordinateurs d'extrémité ouvrant une session avant le 24 septembre 2013 et se connectant aux serveurs de déploiement recevront la nouvelle stratégie et les commandes de programmation.

Tout ordinateur d'extrémité sur lequel la programmation déclenche la commande SGMCMDIntn -WOLstart entre le 24 sept. 2013 à midi et le 25 sept. 2013, à 6 heures du matin se trouve dans l'intervalle de l'éveil par appel réseau et ce dernier sera par conséquent activé.

26 Options de récupération

SafeGuard Enterprise propose plusieurs options de récupération, adaptées à différents scénarios :

- **Récupération de connexion avec Local Self Help**

  Local Self Help permet aux utilisateurs ayant oublié leur mot de passe de se connecter à leur ordinateur sans l'aide du support. Les utilisateurs peuvent accéder de nouveau à leur ordinateur même si aucune connexion téléphonique ou réseau n'est disponible (à bord d'un avion, par exemple). Pour se connecter, ils doivent répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage SafeGuard.

  Local Self Help réduit le nombre d'appels de récupération de connexion, et ainsi les tâches de routine des membres du support en leur permettant de se concentrer sur des demandes plus complexes.

  Retrouvez plus d'informations à la section Récupération avec Local Self Help à la page 218.

- **Récupération avec Challenge/Réponse**

  Le mécanisme Challenge/Réponse est un système de récupération de connexion sécurisé et fiable qui vient en aide aux utilisateurs qui ne peuvent pas se connecter à leur ordinateur ou accéder aux données chiffrées. Lors de la procédure Challenge/Réponse, l'utilisateur communique le code de challenge généré sur l'ordinateur d'extrémité au responsable du support qui générera à son tour un code de réponse. Ce code autorisera l'utilisateur à exécuter une action spécifique sur l'ordinateur d'extrémité.

  Grâce à la récupération par Challenge/Réponse, SafeGuard Enterprise propose plusieurs flux de travail pour les scénarios de récupération types nécessitant l'aide du support.

  Retrouvez plus d'informations à la section Récupération avec Challenge/Réponse à la page 223.

- **Récupération du système pour le chiffrement intégral du disque SafeGuard**

  SafeGuard Enterprise offre différentes méthodes et outils de récupération suite à des problèmes de composants système essentiels et de composants SafeGuard Enterprise, par exemple :

  - MBR (Master Boot Record) corrompu
  - Problèmes de noyau SafeGuard Enterprise
  - Problèmes d'accès aux volumes
  - Problèmes d'initialisation Windows

Retrouvez plus d'informations à la section Récupération du système pour le chiffrement intégral du disque SafeGuard à la page 240.

26.1 Récupération avec Local Self Help

SafeGuard propose Local Self Help afin de permettre à l'utilisateur ayant oublié son mot de passe de se connecter à son ordinateur sans recourir au support technique. Local Self Help réduit le nombre d'appels de récupération de connexion, et ainsi les tâches de routine des membres du support en leur permettant de se concentrer sur des demandes plus complexes.

Grâce à Local Self Help, les utilisateurs peuvent accéder de nouveau à leur ordinateur portable dans les situations où aucune connexion par téléphone ou réseau n'est disponible et où ils ne peuvent donc pas utiliser de procédure Challenge/Réponse (par exemple à bord d'un avion). L'utilisateur peut se connecter à son ordinateur en répondant à un nombre prédéfini de questions dans l'authentification au démarrage SafeGuard.

En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles il faudra répondre et les distribuer sur les ordinateurs d'extrémité dans une stratégie. À titre d'exemple, nous vous proposons un sujet de question prédéfini. Vous pouvez utiliser ce sujet tel quel ou le modifier. Dans la stratégie correspondante, vous pouvez également accorder aux utilisateurs le droit de définir des questions personnalisées.

Lorsque Local Self Help a été activé par la stratégie, un assistant Local Self Help est disponible pour guider les utilisateurs finaux en fournissant les réponses initiales et en modifiant les questions.

La récupération avec Local Self Help est disponible pour les méthodes de connexion suivantes dans l'authentification au démarrage SafeGuard :

- Connexion par identifiant utilisateur et mot de passe
- Connexion par empreinte digitale
- Connexion avec un token non cryptographique dans la mesure où la connexion avec identifiant utilisateur et mot de passe a aussi été activée dans une stratégie du type **Authentification**.

Retrouvez une description détaillée de Local Self Help sur l'ordinateur d'extrémité dans le *Manuel d'utilisation de SafeGuard Enterprise*, au chapitre *Récupération avec Local Self Help*.

26.1.1 Définition des paramètres de Local Self Help dans une stratégie

Définissez les paramètres de Local Self Help dans une stratégie du type **Paramètres généraux** sous **Récupération de connexion** - **Local Self Help**. Vous pouvez activer ici la fonction à utiliser sur l'ordinateur d'extrémité et définir d'autres droits et paramètres.

Activation de Local Self Help

Pour activer Local Self Help et l'utiliser sur l'ordinateur d'extrémité, sélectionnez **Oui** dans le champ **Activer Local Self Help**.

Une fois la stratégie appliquée aux ordinateurs d'extrémité, ce paramètre permet à l'utilisateur d'avoir recours à Local Self Help pour récupérer la connexion. Pour pouvoir utiliser Local Self Help, l'utilisateur doit alors activer cette méthode de récupération en répondant à un nombre de questions spécifié parmi les questions reçues ou en créant et en répondant à des questions personnalisées (en fonction de ses autorisations).

À cet effet, l'Assistant Local Self Help est disponible via une icône dans la barre des tâches Windows une fois la stratégie appliquée et l'ordinateur redémarré.

Configuration de Local Self Help

Vous pouvez définir les options suivantes pour Local Self Help dans une stratégie du type **Paramètres généraux**.

- **Longueur minimum des réponses**

  Définissez la longueur minimale (en caractères) des réponses. Le nombre par défaut est **1**.

- **Texte de bienvenue sous Windows**

  Vous pouvez indiquer le texte d'informations individuel à afficher dans la première boîte de dialogue au démarrage de l'Assistant Local Self Help sur l'ordinateur d'extrémité. Avant de spécifier le texte ici, il doit être créé et enregistré.

- **L'utilisateur peut définir des questions personnalisées**

  Les scénarios suivants sont possibles concernant la définition de questions pour Local Self Help :

  - En tant que responsable de la sécurité, définissez les questions et distribuez-les aux utilisateurs. Les utilisateurs ne sont pas autorisés à définir des questions personnalisées.
  - En tant que responsable de la sécurité, définissez les questions et distribuez-les aux utilisateurs. Les utilisateurs sont également autorisés à définir des questions personnalisées. Lorsqu'ils répondent au nombre minimum de questions nécessaire pour activer Local Self Help, les utilisateurs peuvent choisir entre des questions prédéfinies et des questions personnalisées ou une combinaison des deux.
  - Vous autorisez les utilisateurs à définir des questions personnalisées. Les utilisateurs activent Local Self Help sur leurs ordinateurs en définissant des questions personnalisées et en y répondant.

Pour autoriser les utilisateurs à définir des questions personnalisées, sélectionnez l'option **Oui** dans le champ **L'utilisateur peut définir des questions personnalisées**.

26.1.2 Définition de questions

Pour pouvoir utiliser Local Self Help sur un ordinateur d'extrémité, l'utilisateur doit répondre à un nombre prédéfini de questions et les enregistrer. En tant que responsable de la sécurité avec les droits nécessaires, vous pouvez indiquer le nombre de questions auxquelles l'utilisateur doit répondre pour activer Local Self Help sur l'ordinateur d'extrémité. Vous pouvez également préciser le nombre de questions qui seront aléatoirement sélectionnées dans l'authentification au démarrage SafeGuard. Pour se connecter à l'authentification au démarrage SafeGuard avec Local Self Help, l'utilisateur doit répondre correctement à toutes les questions affichées dans l'authentification au démarrage.

En tant que responsable de la sécurité avec les droits nécessaires, vous pouvez enregistrer et modifier les questions Local Self Help dans SafeGuard Management Center.

26.1.3 Définition du nombre de questions en attente de réponse

Vous pouvez définir le nombre de questions auxquelles il faut répondre lors de la configuration de Local Self Help et dans l'authentification au démarrage SafeGuard.

1. Dans la zone de navigation **Stratégies**, sélectionnez **Questions Local Self Help**.
2. Dans la zone d'action sous **Paramètres Local Self Help**, vous pouvez indiquer deux valeurs différentes pour le nombre de questions Local Self Help :

   a) Dans le champ **Nombre minimum de questions/réponses**, indiquez le nombre de questions auxquelles l'utilisateur doit répondre dans l'assistant Local Self Help pour activer Local Self Help sur l'ordinateur d'extrémité.

      Pour que Local Self Help soit actif, le nombre de questions spécifiées dans ce champ doit être disponible avec les réponses sur l'ordinateur d'extrémité.

   b) Dans le champ **Nombre de questions présentées dans la POA**, indiquez le nombre de questions auxquelles l'utilisateur doit répondre à l'authentification au démarrage SafeGuard lors de la connexion avec Local Self Help.

      Les questions affichées dans l'authentification au démarrage SafeGuard sont sélectionnées de manière aléatoire à partir des questions auxquelles l'utilisateur a répondu dans l'assistant Local Self Help.

   Le nombre spécifié dans le champ **Nombre minimum de questions/réponses** doit être supérieur au nombre indiqué dans le champ **Nombre de questions présentées dans la POA**. Si ce n'est pas le cas, un message d'erreur apparaît lorsque vous enregistrez vos changements.

   Les valeurs par défaut sont :

   - **Nombre minimum de questions/réponses :** 10
   - **Nombre de questions présentées dans la POA :** 5

3. Enregistrez vos changements dans la base de données.

Le nombre de questions s'applique à la configuration de Local Self Help déployée sur les ordinateurs d'extrémité.

26.1.4 Utilisation du modèle

Un sujet de question prédéfini est disponible pour Local Self Help. Ce sujet de question est disponible dans SafeGuard Management Center sous **Questions Local Self Help**.

Vous pouvez utiliser le sujet de question prédéfini tel quel, le modifier ou le supprimer.

26.1.5 Importation de sujets de question

À l'aide de la procédure d'importation, vous pouvez importer vos propres listes de questions créées sous la forme de fichiers .XML.

1. Créez un nouveau sujet de question. Retrouvez plus d'informations à la section Création d'un nouveau sujet de question et ajout de questions à la page 221.
2. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
3. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel du sujet de question. Dans le menu contextuel, sélectionnez **Importer**.
4. Sélectionnez le répertoire et le sujet de question, puis cliquez sur **Ouvrir**.

Les questions importées s'affichent dans la zone d'action. Vous pouvez maintenant enregistrer le sujet de question tel quel ou le modifier.

26.1.6 Création d'un nouveau sujet de question et ajout de questions

Vous pouvez créer de nouveaux sujets de question à propos de thèmes différents. Vous pouvez ainsi proposer aux utilisateurs un choix de sujets de question qui pourraient leur convenir.

1. Dans la zone de navigation **Stratégies**, sélectionnez **Questions Local Self Help**.
2. Cliquez avec le bouton droit de la souris sur **Questions Local Self Help**, puis sélectionnez **Nouveau** > **Sujet de la question**.
3. Saisissez un nom pour le sujet de question et cliquez sur **OK**.
4. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
5. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel du sujet de question. Dans le menu contextuel, sélectionnez **Ajouter**.

   Une nouvelle ligne de question est ajoutée.

6. Saisissez votre question et appuyez sur **Entrée**. Répétez cette étape pour ajouter d'autres questions.
7. Pour enregistrer vos modifications, cliquez sur l'icône **Enregistrer** dans la barre d'outils.

Votre sujet de question est enregistré. Il est automatiquement transféré avec la stratégie du type **Paramètres généraux**, activant Local Self Help sur les ordinateurs d'extrémité.

26.1.7 Modification de sujets de question

1. Dans la zone de navigation **Stratégies**, sélectionnez le sujet de question souhaité sous **Questions Local Self Help**.

2. Vous pouvez maintenant ajouter, modifier ou supprimer des questions.
   - Pour ajouter des questions, cliquez avec le bouton droit de la souris dans la zone d'action pour afficher le menu contextuel. Dans le menu contextuel, cliquez sur **Ajouter**. Une nouvelle ligne est ajoutée à la liste de questions. Entrez votre question sur la ligne.
   - Pour modifier des questions, cliquez sur le texte de la question souhaitée dans la zone d'action. La question est marquée d'une icône en forme de crayon. Entrez vos modifications sur la ligne de la question.
   - Pour supprimer des questions, sélectionnez la question souhaitée en cliquant sur la case grise située au début de la ligne de la question dans la zone d'action, puis cliquez sur **Supprimer** dans le menu contextuel de la question.
3. Pour enregistrer vos modifications, cliquez sur l'icône **Enregistrer** dans la barre d'outils.

Le sujet de question modifié est enregistré. Il est transféré avec la stratégie du type **Paramètres généraux**, activant Local Self Help sur les ordinateurs d'extrémité.

26.1.8 Suppression de sujets de question

Pour supprimer l'intégralité d'un sujet de question, cliquez avec le bouton droit de la souris sur le sujet concerné **Questions Local Self Help** dans la zone de navigation **Stratégies**, puis sélectionnez **Supprimer**.

Remarque : si vous supprimez un sujet de question alors que des utilisateurs ont déjà répondu à certaines questions pour activer Local Self Help sur leurs ordinateurs, leurs réponses ne sont plus valides car les questions n'existent plus.

26.1.9 Enregistrement de textes de bienvenue

Vous pouvez enregistrer un texte de bienvenue à afficher dans la première boîte de dialogue de l'Assistant Local Self Help.

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Management Center. La taille maximale des fichiers de textes d'informations est de 50 Ko. SafeGuard Enterprise utilise les textes codés en Unicode UTF-16 uniquement. Si vous ne créez pas les fichiers texte dans ce format, ils seront automatiquement convertis lorsqu'ils seront enregistrés.

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau** > **Texte**.
2. Saisissez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation **Stratégies.** Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

26.2 Récupération avec Challenge/Réponse

Pour simplifier le flux de travail et réduire les coûts du support, SafeGuard Enterprise fournit une solution de récupération Challenge/Réponse. Grâce au mécanisme convivial Challenge/Réponse, SafeGuard Enterprise aide les utilisateurs qui ne peuvent pas se connecter ou qui ne peuvent pas accéder aux données chiffrées.

Cette fonctionnalité est intégrée au SafeGuard Management Center en tant qu'**Assistant de récupération**.

Avantages de la procédure Challenge/Réponse

Le mécanisme Challenge/Réponse est un système de récupération sécurisé et fiable.

- Tout au long du processus, aucune donnée confidentielle n'est échangée sous une forme autre que chiffrée.
- Cette procédure ne contient aucun point d'écoute électronique de tiers, car les données espionnées ne peuvent pas être utilisées ultérieurement ni sur d'autres périphériques.
- Aucune connexion réseau en ligne n'est nécessaire pour l'ordinateur. L'assistant de code de réponse du support s'exécute également sur un ordinateur d'extrémité non administré sans connexion au serveur SafeGuard Enterprise. Aucune infrastructure complexe n'est nécessaire.
- L'utilisateur peut commencer à retravailler rapidement. L'oubli du mot de passe n'entraîne aucune perte de données chiffrées.

Situations classiques nécessitant l'aide du support

- Un utilisateur a oublié le mot de passe de connexion et l'ordinateur a été verrouillé.
- Un utilisateur a oublié ou perdu le token/carte à puce.
- Le cache local de l'authentification au démarrage SafeGuard est partiellement endommagé.
- Si un utilisateur est absent, ses collègues doivent pouvoir accéder aux données de son ordinateur.
- Un utilisateur souhaite accéder à un volume chiffré à l'aide d'une clé qui n'est pas disponible sur l'ordinateur.

SafeGuard Enterprise propose différents flux de travail de récupération pour ces scénarios types, ce qui permet aux utilisateurs d'accéder de nouveau à leurs ordinateurs.

26.2.1 Flux de travail Challenge/Réponse

La procédure Challenge/Réponse repose sur les deux composants suivants :

- L'ordinateur d'extrémité sur lequel le code de challenge est généré.

- SafeGuard Management Center où, en tant que responsable du support possédant les droits correspondants, vous créez un code de réponse qui autorisera l'utilisateur à effectuer l'action requise sur l'ordinateur.

  Remarque : pour une procédure Challenge/Réponse, vous avez besoin des droits d'**Accès complet** pour les ordinateurs/utilisateurs concernés.

1. Sur l'ordinateur d'extrémité, l'utilisateur demande le code de challenge. En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage SafeGuard, soit dans l'outil de récupération de clé KeyRecovery.

   Un code de challenge sous la forme d'une chaîne de caractères ASCII est généré puis affiché.

2. L'utilisateur contacte le support technique et leur fournit l'identification nécessaire et le code de challenge.
3. Le support lance l'assistant de récupération dans SafeGuard Management Center.
4. Le support sélectionne le type de récupération approprié, confirme les informations d'identification et le code de challenge, puis sélectionne l'action de récupération souhaitée.

   Un code de réponse sous la forme d'une chaîne de caractères ASCII est généré et s'affiche.

5. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou SMS.
6. L'utilisateur saisit le code de réponse, En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage SafeGuard, soit dans l'outil de récupération de clé KeyRecovery.

   L'utilisateur est ensuite autorisé à effectuer l'action convenue, par exemple à réinitialiser le mot de passe et à reprendre son travail.

26.2.2 Exigences liées au changement du mot de passe de l'utilisateur

Dans le cadre du processus de récupération de SafeGuard Enterprise, les utilisateurs peuvent être contraints de changer leurs mots de passe Windows. Le tableau suivant fournit des informations sur les cas dans lesquels un changement de mot de passe est requis. Les quatre premières colonnes indiquent les conditions spécifiques pouvant se produire lors de la procédure Challenge/Réponse. La dernière colonne indique si l'utilisateur est contraint de changer son mot de passe Windows, en fonction des conditions indiquées dans les colonnes précédentes.

Condition : procédure C/R générée avec connexion de l'utilisateur et affichage de l'option du mot de passe	Condition : procédure C/R générée avec connexion de l'utilisateur	Condition : contrôleur de domaine disponible	Condition : affichage du mot de passe refusé par l'utilisateur	Résultat : l'utilisateur est contraint de changer son mot de passe Windows
Oui	Oui	Oui	Non	**Non**

Condition : procédure C/R générée avec connexion de l'utilisateur et affichage de l'option du mot de passe	Condition : procédure C/R générée avec connexion de l'utilisateur	Condition : contrôleur de domaine disponible	Condition : affichage du mot de passe refusé par l'utilisateur	Résultat : l'utilisateur est contraint de changer son mot de passe Windows
Oui	Oui	Oui	Oui	**Oui**
Oui	Oui	Non	Oui	**Non**
Non	Oui	Oui	Non disponible	**Oui**
Non	Oui	Non	Non disponible	**Non**
Non	Non	Non	Non disponible	**Non**

26.2.3 Lancement de l'assistant de récupération

Pour pouvoir effectuer une procédure de récupération, assurez-vous de disposer des droits et des autorisations requis.

1. Connectez-vous au SafeGuard Management Center.
2. Cliquez sur **Outils** > **Récupération** dans la barre de menus.

L'**Assistant de récupération** démarre. Vous pouvez sélectionner le type de récupération que vous souhaitez utiliser.

26.2.4 Types de récupération

Sélectionnez le type de récupération que vous souhaitez utiliser. Les types de récupération suivants sont fournis :

- **Clients SafeGuard Enterprise administrés**

  Procédure Challenge/Réponse pour ordinateurs d'extrémité administrés de façon centralisée par SafeGuard Management Center. Ils sont répertoriés dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center.

- **Clients virtuels**

  En cas de situation de récupération complexe, par exemple lorsque l'authentification au démarrage SafeGuard est corrompue, l'accès aux données chiffrées peut être facilement récupéré grâce à la procédure Challenge/Réponse. Dans ce cas, des fichiers spécifiques appelés clients virtuels sont utilisés. Ce type est disponible pour les ordinateurs administrés et non administrés.

- **Clients Sophos SafeGuard autonomes**

  Challenge/Réponse pour les ordinateurs non administrés. Ils ne sont jamais connectés au serveur SafeGuard Enterprise. Les informations de récupération requises sont basées sur

le fichier de récupération de clé. Sur chaque ordinateur d'extrémité, ce fichier est généré lors du déploiement du logiciel de chiffrement Sophos SafeGuard. Pour assurer la procédure Challenge/Réponse dans ce cas, le fichier de récupération de clé doit être accessible pour le support technique Sophos SafeGuard, par exemple sur un chemin réseau partagé.

Remarque : par ailleurs, la méthode de récupération de connexion Local Self Help ne requiert aucune assistance du support.

26.2.5 Procédure Challenge/Réponse pour clients SafeGuard Enterprise (administrés)

SafeGuard Enterprise fournit la procédure de récupération aux ordinateurs d'extrémité SafeGuard Enterprise enregistrés dans la base de données, dans différents scénarios de récupération, par exemple la récupération de mots de passe.

La procédure Challenge/Réponse est prise en charge pour les ordinateurs natifs SafeGuard Enterprise et les ordinateurs d'extrémité chiffrés BitLocker. Le système détermine dynamiquement quel type d'ordinateur est en cours d'utilisation. Le flux de travail de récupération est ajusté en conséquence.

26.2.5.1 Actions de récupération pour les clients SafeGuard Enterprise

Le flux de travail de récupération dépend du type d'ordinateur d'extrémité pour lequel une récupération est demandée.

Remarque : s'il s'agit d'ordinateurs chiffrés BitLocker, la seule action de récupération consiste à récupérer la clé utilisée pour chiffrer un volume spécifique. La récupération de mots de passe n'est pas proposée.

26.2.5.1.1 Récupération du mot de passe à l'authentification au démarrage SafeGuard

L'un des scénarios les plus courants est l'oubli du mot de passe par l'utilisateur. Par défaut, SafeGuard Enterprise est installé avec l'authentification au démarrage SafeGuard activée. Le mot de passe de l'authentification au démarrage SafeGuard permettant d'accéder à l'ordinateur est identique au mot de passe Windows.

Si l'utilisateur a oublié le mot de passe à l'authentification au démarrage SafeGuard, le responsable du support SafeGuard Enterprise peut générer une réponse pour **Initialiser le client SGN avec une connexion utilisateur**, mais sans afficher le mot de passe de l'utilisateur. Par contre, dans ce cas, après avoir entré le code de réponse, l'ordinateur démarre sur le système d'exploitation. L'utilisateur doit changer le mot de passe lors de la connexion à Windows (à condition que le domaine soit accessible). L'utilisateur peut alors se connecter à Windows ainsi qu'à l'authentification au démarrage SafeGuard à l'aide du nouveau mot de passe.

26.2.5.1.2 Bon usage de récupération du mot de passe à l'authentification au démarrage SafeGuard

Nous vous conseillons d'utiliser les méthodes suivantes pour récupérer un mot de passe oublié par l'utilisateur afin d'éviter que ce mot de passe ne soit réinitialisé de manière centralisée :

- **Utilisation de Local Self Help.**

  Avec la récupération avec Local Self Help, le mot de passe actuel peut être affiché et l'utilisateur peut continuer à l'utiliser sans devoir le réinitialiser et sans requérir l'assistance du support.

- **Utilisation de la procédure Challenge/Réponse pour les clients SafeGuard Enterprise (administrés) :**

  Nous vous recommandons d'éviter de réinitialiser le mot de passe dans Active Directory avant la procédure Challenge/Réponse. Cela garantit que le mot de passe reste synchronisé entre Windows et SafeGuard Enterprise. Assurez-vous que le support Windows en a bien connaissance.

En tant que responsable du support de SafeGuard Enterprise, générez une réponse pour **Initialiser le client SGN avec une connexion utilisateur** à l'aide de l'option **Afficher le mot de passe utilisateur**. Ceci est utile car il n'est pas nécessaire de réinitialiser le mot de passe dans l'Active Directory. L'utilisateur peut continuer à travailler avec l'ancien mot de passe et le modifier localement par la suite.

26.2.5.1.3 Affichage du mot de passe utilisateur

SafeGuard Enterprise permet aux utilisateurs d'afficher leur mot de passe lors de la procédure Challenge/Réponse. Ceci est utile car il n'est pas nécessaire de réinitialiser le mot de passe dans l'Active Directory. Cette option est disponible uniquement si l'action **Initialiser le client SGN avec une connexion utilisateur** est demandée.

26.2.5.1.4 Un autre utilisateur doit démarrer l'ordinateur protégé par SafeGuard Enterprise

Dans ce cas, l'utilisateur qui doit accéder à l'ordinateur démarre ce dernier et saisit son nom d'utilisateur. L'utilisateur demande alors un challenge. Le support SafeGuard génère une réponse du type **Initialiser le client SGN sans connexion utilisateur** et **Connexion automatique vers Windows** activée. L'utilisateur est connecté et peut utiliser l'ordinateur.

26.2.5.1.5 Restauration de la mémoire cache de la stratégie SafeGuard Enterprise

Cette procédure est nécessaire si le cache de stratégies SafeGuard est endommagé. Le cache local stocke toutes les clés et stratégies ainsi que les certificats utilisateur et les fichiers d'audit. Lorsque le cache local est corrompu, la récupération de connexion est désactivée par défaut. Sa restauration s'effectue automatiquement à partir de la sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local. Si le cache local doit être réparé à l'aide de la procédure Challenge/Réponse, la récupération de connexion peut être activée par stratégie. Dans ce cas, l'utilisateur est automatiquement invité à lancer une procédure Challenge/Réponse, si le cache local est corrompu.

26.2.5.1.6 SafeGuard Data Exchange : récupération d'un mot de passe oublié

SafeGuard Data Exchange sans le chiffrement de périphériques ne fournit pas la récupération Challenge/Réponse, lorsque l'utilisateur a oublié son mot de passe. Dans ce cas, vous devez changer le mot de passe dans Active Directory. Connectez-vous à l'ordinateur d'extrémité sans le fournisseur de codes d'accès Sophos et restaurez la configuration utilisateur sur l'ordinateur d'extrémité.

26.2.5.2 Réponse pour les clients SafeGuard Enterprise

1. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise (administré)**.
2. Sous **Domaine**, sélectionnez le domaine requis dans la liste.

3. Sous **Ordinateur**, saisissez ou sélectionnez le nom d'ordinateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :

   - Pour sélectionner un nom, cliquez sur [**...**]. Cliquez ensuite sur **Rechercher maintenant**. Une liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur apparaît sur la page **Type de récupération**.
   - Entrez le nom écourté de l'ordinateur directement dans le champ. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.
   - Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

     CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae

4. Cliquez sur **Suivant**.
5. Sélectionnez le domaine de l'utilisateur.
6. Saisissez le nom de l'utilisateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :

   - Pour sélectionner le nom utilisateur, cliquez sur [**...**] dans la section **Informations utilisateur** de la page **Récupération de connexion**. Cliquez ensuite sur **Rechercher maintenant**. La liste des utilisateurs s'affiche. Sélectionnez le nom requis, puis cliquez sur **OK**. Le nom utilisateur apparaît sur la page **Type de récupération**.
   - Saisissez directement le nom de l'utilisateur. Assurez-vous de l'orthographier correctement.

7. Cliquez sur **Suivant**.

   Une fenêtre apparaît où vous pouvez saisir le code de challenge.

8. Saisissez le code de challenge que l'utilisateur vous a transmis et cliquez sur **Suivant**. Ce code est vérifié. Si le code a été saisi de façon incorrecte, le terme **Challenge non valide** apparaît au-dessous du bloc contenant l'erreur.
9. Si le code de challenge a été saisi correctement, l'action de récupération demandée par le client SafeGuard Enterprise, ainsi que les actions de récupération possibles sur ce client s'affichent. Les actions possibles pour la réponse dépendent des actions demandées côté client lors de l'appel du challenge. Par exemple, si l'action **token cryptographique demandé** nécessaire est requise côté client, les actions disponibles pour la réponse sont **Initialiser le client SGN avec une connexion utilisateur** et **Initialiser le client SGN sans connexion utilisateur**.
10. Sélectionnez l'action que l'utilisateur doit exécuter.
11. Si l'action **Initialiser le client SGN avec une connexion utilisateur** a été sélectionnée, vous pouvez également sélectionner **Afficher le mot de passe utilisateur** afin d'afficher le mot de passe sur l'ordinateur cible.
12. Cliquez sur **Suivant**.
13. Un code de réponse est généré. Fournissez le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L'utilisateur peut saisir le code de réponse sur l'ordinateur d'extrémité et exécuter l'action autorisée.

26.2.5.3 Réponse pour les clients SafeGuard Enterprise chiffrés BitLocker - ordinateurs d'extrémité UEFI

Pour les ordinateurs d'extrémité UEFI satisfaisant à certaines conditions requises, SafeGuard Enterprise offre la procédure Challenge / Réponse pour la récupération. Sur les ordinateurs d'extrémité UEFI qui ne remplissent pas ces conditions requises, la gestion SafeGuard BitLocker sans procédure Challenge/Réponse est installée automatiquement. Retrouvez plus d'informations sur la récupération de ces ordinateurs d'extrémité à la section Clé de récupération pour les clients SafeGuard Enterprise chiffrés par BitLocker - ordinateurs d'extrémité BIOS à la page 229.

1. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise** (**administré**).
2. Sous **Domaine**, sélectionnez le domaine requis dans la liste.
3. Sous **Ordinateur**, saisissez ou sélectionnez le nom d'ordinateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Pour sélectionner un nom, cliquez sur [**...**]. Cliquez ensuite sur **Rechercher maintenant**. Une liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur apparaît sur la page **Type de récupération**.
   - Entrez le nom écourté de l'ordinateur directement dans le champ. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.
   - Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

     `CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae`
4. Cliquez sur **Suivant**.
5. Sélectionnez le volume auquel accéder dans la liste et cliquez sur **Suivant**.
6. Cliquez sur **Suivant**.

   Une fenêtre apparaît où vous pouvez saisir le code de challenge.
7. Saisissez le code de challenge que l'utilisateur vous a transmis et cliquez sur **Suivant**.
8. Un code de réponse est généré. Fournissez le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L'utilisateur peut saisir le code de réponse et accéder de nouveau à l'ordinateur d'extrémité.

26.2.5.4 Clé de récupération pour les clients SafeGuard Enterprise chiffrés par BitLocker - ordinateurs d'extrémité BIOS

S'il s'agit d'ordinateurs BIOS chiffrés BitLocker, un volume qui n'est plus accessible peut être récupéré.

1. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise** (**administré**).
2. Sous **Domaine**, sélectionnez le domaine requis dans la liste.

3. Sous **Ordinateur**, saisissez ou sélectionnez le nom d'ordinateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Pour sélectionner un nom, cliquez sur [**...**] Cliquez ensuite sur **Rechercher maintenant**. Une liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur s'affiche dans la fenêtre **Type de récupération** sous **Domaine**.
   - Entrez le nom écourté de l'ordinateur directement dans le champ. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.
   - Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

     `CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae`
4. Cliquez sur **Suivant**.
5. Sélectionnez le volume auquel accéder dans la liste et cliquez sur **Suivant**.
6. L'assistant de récupération affiche la clé de récupération à 48 chiffres correspondante.
7. Fournissez cette clé à l'utilisateur.

L'utilisateur peut la saisir afin de récupérer le volume chiffré BitLocker sur l'ordinateur d'extrémité.

26.2.5.5 Clé de récupération pour les clients SafeGuard Enterprise chiffrés par FileVault 2 - ordinateurs d'extrémité Mac

S'il s'agit de Macs chiffrés FileVault 2, un volume qui n'est plus accessible peut être récupéré.

1. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise** (**administré**).
2. Sous **Domaine**, sélectionnez le domaine requis dans la liste.
3. Sous **Ordinateur**, saisissez ou sélectionnez le nom d'ordinateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Pour sélectionner un nom, cliquez sur [**...**] Cliquez ensuite sur **Rechercher maintenant**. Une liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur s'affiche dans la fenêtre **Type de récupération** sous **Domaine**.
   - Entrez le nom écourté de l'ordinateur directement dans le champ. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.
   - Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

     `CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae`
4. Cliquez sur **Suivant**.
5. L'assistant de récupération affiche la clé de récupération à 24 chiffres correspondante.
6. Fournissez cette clé à l'utilisateur.

L'utilisateur peut la saisir afin de récupérer le volume chiffré FileVault 2 sur l'ordinateur d'extrémité.

26.2.6 Challenge/Réponse à l'aide de clients virtuels

Grâce à la récupération des clients virtuels, SafeGuard Enterprise permet de récupérer des volumes chiffrés même dans des situations d'urgence complexes, par exemple lorsque l'authentification au démarrage SafeGuard est corrompue. Elle s'applique aussi bien aux ordinateurs d'extrémité administrés qu'aux ordinateurs administrés non administrés.

Remarque : la récupération des clients virtuels doit uniquement être utilisée pour résoudre des situations d'urgence complexes. Si, par exemple, une seule clé manque pour la récupération d'un volume, la meilleure solution consiste à affecter tout simplement la clé manquante au jeu de clés de l'utilisateur approprié.

26.2.6.1 Flux de travail de récupération à l'aide de clients virtuels

Pour accéder à l'ordinateur d'extrémité chiffré, la procédure ci-dessous s'applique :

1. Demandez au support technique de vous fournir le disque de récupération SafeGuard Enterprise.

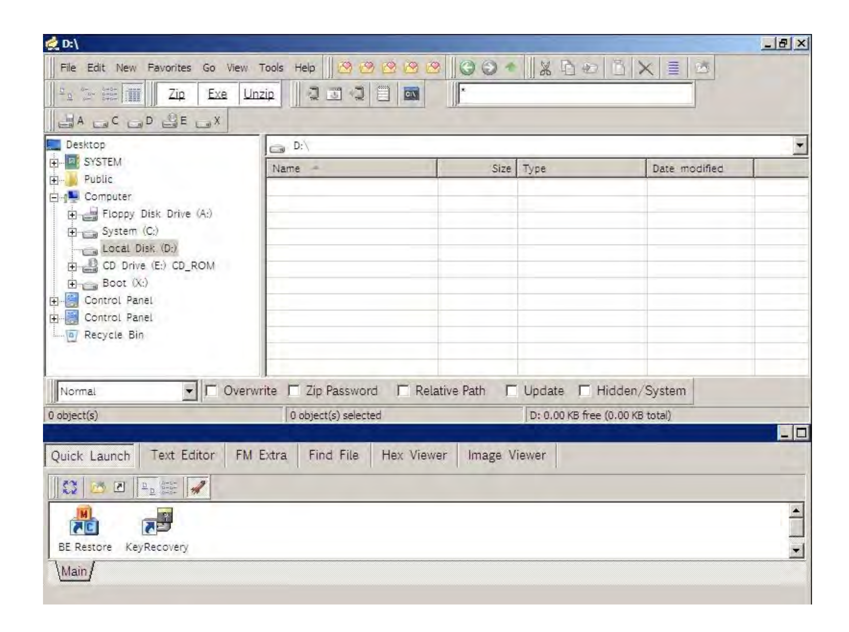
   Le support peut télécharger le disque de récupération Windows PE avec les derniers pilotes du filtre SafeGuard Enterprise sur le site du support Sophos. Retrouvez plus d'informations sur : http://www.sophos.com/fr-fr/support/knowledgebase/108805.aspx.
2. Créez le client virtuel dans SafeGuard Management Center. Retrouvez plus d'informations à la section Création de clients virtuels à la page 64.
3. Exportez le client virtuel dans un fichier. Retrouvez plus d'informations à la section Exportation de clients virtuels à la page 64.
4. Vous avez aussi la possibilité d'exporter plusieurs clés de client virtuel dans un fichier. Retrouvez plus d'informations à la section Création et exportation de fichiers de clés pour la récupération des clients virtuels à la page 65.
5. Démarrez l'ordinateur d'extrémité depuis le disque de récupération.
6. Importez le fichier du client virtuel dans l'outil de récupération de clé KeyRecovery.
7. Initialisez le challenge dans l'outil de récupération de clé KeyRecovery.
8. Confirmez le client virtuel dans SafeGuard Management Center.
9. Sélectionnez l'action de récupération requise.
10. Saisissez le code de challenge dans SafeGuard Management Center.
11. Saisissez le code de réponse dans SafeGuard Management Center.
12. Saisissez le code de réponse dans l'outil de récupération de clé KeyRecovery.

L'ordinateur est de nouveau accessible.

26.2.6.2 Démarrage de l'ordinateur depuis le disque de récupération

Condition préalable : Vérifiez que la séquence d'initialisation dans les paramètres du BIOS permet de démarrer à partir du CD.

1. Insérez le disque de récupération, puis démarrez l'ordinateur d'extrémité. Le gestionnaire de fichiers intégré s'ouvre. Les volumes et les lecteurs présents s'affichent immédiatement.



Le contenu du lecteur chiffré ne s'affiche pas dans le gestionnaire de fichiers. Ni le système de fichiers, ni la capacité et l'espace utilisé/libre ne figurent dans les propriétés du lecteur chiffré.

2. Au bas du gestionnaire de fichiers, dans la section **Lancement rapide**, cliquez sur l'icône KeyRecovery pour ouvrir l'outil de récupération de clé KeyRecovery. L'outil de récupération de clé KeyRecovery affiche l'identifiant de clé des lecteurs chiffrés.



3. Recherchez l'identifiant de clé des lecteurs auxquels vous souhaitez accéder. Vous devrez fournir cet identifiant de clé ultérieurement.

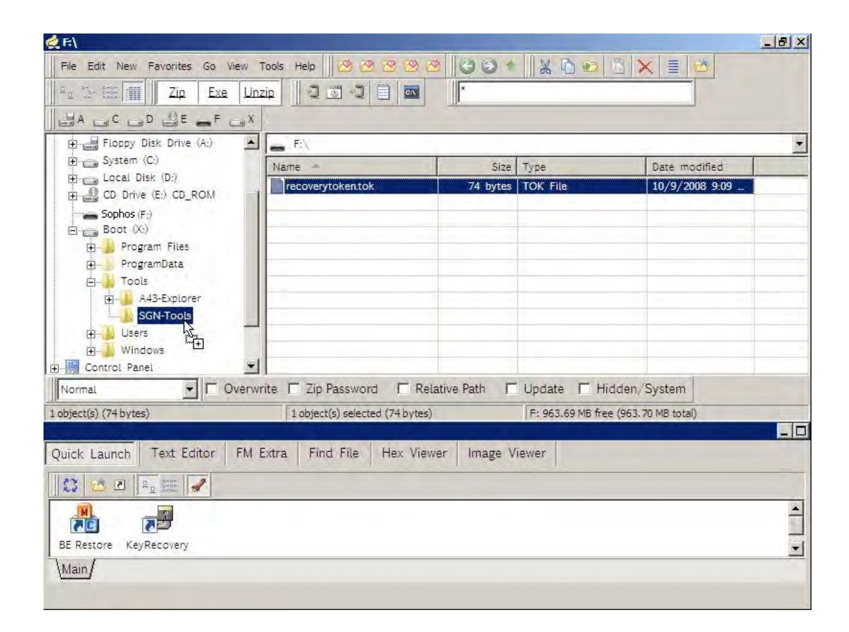
Importez ensuite le client virtuel dans l'outil de récupération de clé.

26.2.6.3 Importation du client virtuel dans l'outil de récupération de clé KeyRecovery

Condition préalable :

- L'ordinateur a été démarré depuis le disque de récupération.
- Vérifiez que le lecteur USB, sur lequel est enregistré le fichier du client virtuel **`recoverytoken.tok`**, a été correctement monté.

1. Dans le gestionnaire de fichiers Windows PE, sélectionnez le lecteur sur lequel est enregistré le client virtuel. Le fichier recoverytoken.tok apparaît sur la droite.
2. Sélectionnez le fichier recoverytoken.tok et faites-le glisser sur le lecteur où se trouve l'outil de récupération de clé KeyRecovery. Déposez-le dans le répertoire Tools\SGN-Tools.



26.2.6.4 Initialisation du challenge dans l'outil de récupération de clé KeyRecovery

1. Au bas du gestionnaire de fichiers Windows PE, dans la section **Lancement rapide**, cliquez sur l'icône KeyRecovery pour ouvrir l'outil de récupération de clé KeyRecovery. L'outil KeyRecovery affiche les ID de clé des lecteurs chiffrés.

   Cet outil démarre et affiche une liste de tous les volumes, ainsi que des informations de chiffrement correspondantes (ID de clé).



2. Sélectionnez le volume à déchiffrer, puis cliquez sur **Importer par C/R** pour générer le code de challenge.

   À titre de référence dans la base de données SafeGuard Enterprise, le fichier client virtuel est utilisé et mentionné dans la procédure Challenge. Le code de challenge est alors généré et s'affiche.

3. Communiquez le nom du client virtuel et le code de challenge au support, par exemple par téléphone ou en envoyant un message texte. Une aide à l'épellation est fournie.

26.2.6.5 Confirmation du client virtuel

Condition préalable : le client virtuel doit avoir été créé dans le SafeGuard Management Center dans **Clients virtuels** ainsi qu'être disponible dans la base de données.

1. Pour ouvrir l'Assistant de récupération dans le SafeGuard Management Center, cliquez sur **Outils** > **Récupération**.
2. Dans **Type de récupération**, sélectionnez **Client virtuel**.
3. Saisissez le nom du client virtuel que l'utilisateur vous a indiqué. Pour ce faire, vous pouvez procéder de plusieurs façons :

   - Saisissez directement le nom unique.
   - Sélectionnez un nom en cliquant sur **[...]** dans la section **Client virtuel** de la boîte de dialogue **Type de récupération**. Cliquez ensuite sur **Rechercher maintenant**. La liste des clients virtuels s'affiche. Sélectionnez le client virtuel requis, puis cliquez sur **OK**. Le nom du client virtuel s'affiche alors sur la page **Type de récupération** sous **Client virtuel**.

4. Cliquez sur **Suivant** pour confirmer le nom du fichier du client virtuel.

Ensuite, sélectionnez l'action de récupération requise.

26.2.6.6 Sélection de l'action de récupération requise

1. Sur la page **Client virtuel**, **Action requise**, sélectionnez l'une des options suivantes :

   - Sélectionnez **Clé requise** pour récupérer une clé unique pour accéder à un volume chiffré sur l'ordinateur.

     Cette option est disponible pour les ordinateurs d'extrémité non administrés et administrés.

   - Sélectionnez **Mot de passe du fichier de clé demandé** pour récupérer plusieurs clés et accéder aux volumes chiffrés sur l'ordinateur. Les clés sont stockées dans un fichier, chiffré par un mot de passe aléatoire enregistré dans la base de données. Ce mot de passe est propre à chaque fichier de clé créé. Le mot de passe figurant dans le code de réponse est transféré sur l'ordinateur cible.

     Cette option est uniquement disponible pour les ordinateurs d'extrémité administrés.

2. Cliquez sur **Suivant**.

26.2.6.7 Sélection de la clé requise (clé unique)

Condition préalable :

Sélectionnez au préalable le client virtuel requis dans l'assistant de récupération du SafeGuard Management Center et l'action de récupération **Clé requise**.

1. Dans l'Assistant de récupération, sur la page **Client virtuel**, sélectionnez si l'action est demandée par un ordinateur d'extrémité administré ou non administré :

   - Pour les ordinateurs d'extrémité administrés, sélectionnez **Clé de récupération du client SafeGuard Enterprise administré**. Cliquez sur [**...**]. Dans **Rechercher des clés**, vous pouvez afficher les clés en fonction de leur ID ou de leur nom symbolique. Cliquez sur **Rechercher maintenant**, sélectionnez la clé et cliquez sur **OK**.

     Remarque : une réponse ne peut être initiée que pour des clés attribuées. Si une clé est inactive, c'est-à-dire qu'elle n'est pas attribuée à au moins un utilisateur, une réponse pour client virtuel est impossible. Dans ce cas, la clé inactive peut être attribuée à un autre utilisateur et une réponse pour cette clé peut être de nouveau générée.

   - Pour les ordinateurs d'extrémité administrés, sélectionnez **Clé de récupération du client Sophos SafeGuard autonome**. Cliquez sur [**...**] près de cette option pour rechercher le fichier. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml. Sélectionnez le fichier et cliquez sur **Ouvrir**.

     Remarque : le support doit pouvoir accéder au fichier de récupération de clé nécessaire pour récupérer l'accès à l'ordinateur. Ce fichier peut par exemple se trouver sur un partage réseau.

2. Cliquez sur **Suivant**. La page pour la saisie du code de challenge apparaît.

La clé requise est transférée vers l'environnement de l'utilisateur, dans le code de réponse.

26.2.6.8 Sélection de la clé requise (plusieurs clés)

Condition préalable :

Cette option est uniquement disponible pour les ordinateurs d'extrémité administrés.

Sélectionnez au préalable le fichier de clé dans le SafeGuard Management Center, sous **Clés et certificats**. En outre, le mot de passe de chiffrement du fichier de clé doit être stocké dans la base de données.

Sélectionnez au préalable le fichier du client virtuel requis dans l'assistant de récupération du SafeGuard Management Center et l'action de récupération **Mot de passe du fichier de clé demandé**.

1. Pour sélectionner un fichier de clé, cliquez sur [**...**] près de cette option. Dans **Fichier de clé**, cliquez sur **Rechercher maintenant**. Sélectionnez le fichier de clé et cliquez sur **OK**.
2. Pour confirmer, cliquez sur **Suivant**.

La page pour la saisie du code de challenge apparaît.

26.2.6.9 Saisie du code de challenge et génération du code de réponse

Condition préalable :

Sélectionnez au préalable le client virtuel requis dans l'assistant de récupération du SafeGuard Management Center et l'action de récupération requise.

1. Saisissez le code de challenge que l'utilisateur vous a transmis et cliquez sur **Suivant**. Ce code est vérifié.

   Si le code de challenge a été saisi correctement, le code de réponse est généré. Si le code a été saisi de façon incorrecte, le terme **Challenge non valide** apparaît au-dessous du bloc contenant l'erreur.

2. Lisez alors le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

Lorsque vous avez sélectionné **Clé requise** comme action de récupération, la clé requise est transférée dans l'environnement utilisateur dans le code de réponse.

Lorsque vous avez sélectionné **Mot de passe du fichier de clé requis** comme action de récupération, le mot de passe du fichier de clé chiffré est transféré dans le code de réponse. Ce fichier de clé est ensuite supprimé.

26.2.6.10 Saisie du code de réponse dans l'outil KeyRecovery

1. Sur l'ordinateur d'extrémité, dans l'outil de récupération de clé KeyRecovery, saisissez le code de réponse fourni par le support.

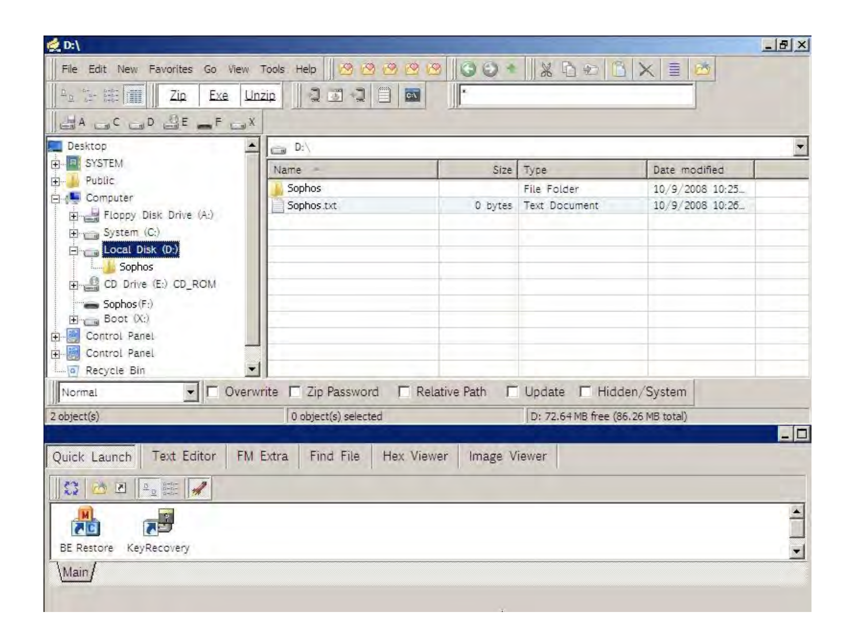
   La clé ou le mot de passe requis pour le fichier de clé figure dans ce code de réponse.



2. Cliquez sur **OK**. Le disque sélectionné pour la procédure Challenge/Réponse a été déchiffré.



3. Pour vérifier si le déchiffrement a réussi, sélectionnez le lecteur déchiffré dans le gestionnaire de fichiers Windows PE :



Le contenu du lecteur déchiffré s'affiche dans le gestionnaire de fichiers. Le système de fichiers, ainsi que la capacité et l'espace utilisé/libre, figurent dans les propriétés du lecteur déchiffré.

L'accès aux données stockées sur cette partition est récupéré. Suite à ce déchiffrement réussi, vous pouvez lire, écrire et copier des données à partir du disque indiqué ou vers celui-ci.

26.2.7 Procédure Challenge/Réponse pour clients Sophos SafeGuard (autonomes)

SafeGuard Enterprise propose aussi une procédure Challenge/Réponse pour les ordinateurs d'extrémité non administrés (clients Sophos SafeGuard autonomes), lorsque l'utilisateur a oublié son mot de passe ou s'il l'a saisi de manière incorrecte un trop grand nombre de fois.

Les ordinateurs non administrés ne disposent d'aucune connexion, même temporaire, au serveur SafeGuard Enterprise. Ils fonctionnent en mode autonome.

Dans ce cas, les informations de récupération nécessaires à la procédure Challenge/Réponse sont basées sur le fichier de récupération de clé. Sur chaque ordinateur d'extrémité non administré, ce fichier de récupération de clé est généré lors du déploiement du logiciel de chiffrement SafeGuard Enterprise. Le fichier de récupération de clé doit être accessible pour le support technique Sophos SafeGuard, par exemple sur un chemin réseau partagé.

Afin de faciliter la recherche et le regroupement des fichiers de récupération, ils portent le nom de l'ordinateur : **`nomordinateur.GUID.xml`** dans leurs noms de fichier. Vous pouvez ainsi effectuer des recherches de caractères génériques avec des astérisques (*), par exemple : *.GUID.xml.

Remarque : lorsqu'un ordinateur est renommé, le cache local de l'ordinateur n'applique pas le changement de nom. Le cache local stocke toutes les clés et stratégies ainsi que les certificats utilisateur et les fichiers d'audit. Le nouveau nom de l'ordinateur doit donc être supprimé du cache local afin de ne conserver que le nom précédent, bien que l'ordinateur ait été renommé sous Windows.

26.2.7.1 Actions de récupération pour les clients Sophos SafeGuard (autonomes)

La procédure Challenge/Réponse pour un ordinateur d'extrémité non administré intervient dans les situations suivantes :

- L'utilisateur a saisi un mot de passe incorrect un trop grand nombre de fois.
- L'utilisateur a oublié le mot de passe.
- Un cache local endommagé doit être réparé.

Aucune clé utilisateur n'est disponible dans la base de données pour les ordinateurs d'extrémité non administrés. Par conséquent, la seule action de récupération possible dans une session de Challenge/Réponse est **Initialisation du client SGN sans connexion utilisateur**.

La procédure Challenge/Réponse permet à l'ordinateur de démarrer à partir de l'authentification au démarrage SafeGuard. L'utilisateur peut alors se connecter à Windows.

Études de cas de récupération potentiels :

L'utilisateur a saisi un mot de passe incorrect un trop grand nombre de fois au niveau de l'authentification au démarrage SafeGuard et l'ordinateur est verrouillé. Mais l'utilisateur connait encore le mot de passe.

L'ordinateur est verrouillé et l'utilisateur est invité à lancer une procédure Challenge/Réponse pour le déverrouiller. Comme l'utilisateur connait le mot de passe correct, il n'est pas nécessaire de le réinitialiser. La procédure Challenge/Réponse permet à l'ordinateur de démarrer à partir de l'authentification au démarrage SafeGuard. L'utilisateur peut ensuite saisir le mot de passe correctement dans la boîte de dialogue de connexion Windows et s'y connecter.

L'utilisateur a oublié le mot de passe

Remarque : nous vous conseillons d'utiliser Local Self Help pour récupérer un mot de passe oublié. Local Self Help permet aux utilisateurs d'avoir leurs mots de passe en cours affichés et de continuer à l'utiliser. Ceci lui évite d'avoir à réinitialiser le mot de passe ou de demander de l'aide au support technique.

Lors de la récupération d'un mot de passe oublié via la procédure Challenge/Réponse, une réinitialisation de mot de passe est requise.

1. La procédure Challenge/Réponse permet à l'ordinateur de démarrer à partir de l'authentification au démarrage SafeGuard.
2. Dans la boîte de dialogue de connexion Windows, l'utilisateur ne connait pas le mot de passe correct. Le mot de passe doit être redéfini au niveau de Windows. Cela nécessite d'autres actions de récupération sortant du périmètre de SafeGuard Enterprise, via des moyens Windows standard.

   Remarque : nous vous recommandons d'éviter la réinitialisation centralisée du mot de passe avant la procédure Challenge/Réponse. Cela garantit que le mot de passe reste synchronisé entre Windows et SafeGuard Enterprise. Assurez-vous que le support Windows en a bien connaissance.

   Nous recommandons les méthodes de réinitialisation de mot de passe Windows suivantes.

   - À l'aide d'un compte de service ou administrateur disponible sur l'ordinateur d'extrémité avec les droits Windows requis.
   - À l'aide d'un disque de réinitialisation de mot de passe Windows sur l'ordinateur d'extrémité.

     En tant que responsable du support, vous pouvez informer l'utilisateur de la procédure à appliquer et lui fournir les codes d'accès Windows supplémentaires ou le disque requis.
3. L'utilisateur saisit le nouveau mot de passe que le support a réinitialisé au niveau de Windows. L'utilisateur doit ensuite modifier ce mot de passe immédiatement en choisissant une valeur connue de lui seul. Un nouveau certificat utilisateur est créé en fonction du nouveau choix de mot de passe Windows. L'utilisateur peut donc se reconnecter à l'ordinateur ainsi qu'à l'authentification au démarrage SafeGuard à l'aide du nouveau mot de passe.

   Remarque : Clés pour SafeGuard Data Exchange : Lorsqu'un mot de passe est réinitialisé et qu'un nouveau certificat est créé, les clés locales précédemment créées pour SafeGuard Data Exchange peuvent être encore utilisées si l'ordinateur d'extrémité est membre d'un domaine. Si le système d'extrémité est membre d'un groupe de travail, l'utilisateur doit se rappeler de la phrase secrète SafeGuard Data Exchange pour réactiver ces clés locales.

Le cache local doit être réparé.

Le cache local stocke toutes les clés et stratégies ainsi que les certificats utilisateur et les fichiers d'audit. Lorsque le cache local est corrompu, la récupération de connexion est désactivée par défaut, c'est-à-dire que sa restauration s'effectue automatiquement à partir de la sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local. En revanche, la récupération de connexion peut être activée par stratégie, si le cache local doit effectivement être réparé avec une procédure Challenge/Réponse. Dans ce cas, l'utilisateur est automatiquement invité à lancer une procédure Challenge/Réponse, si le cache local est corrompu.

26.2.7.2 Génération d'une réponse pour les ordinateurs non administrés à l'aide du fichier de récupération de clé

Remarque : le fichier de récupération de clé généré durant l'installation du logiciel de chiffrement SafeGuard Enterprise doit être stocké dans un emplacement accessible au responsable support et son nom doit être connu.

1. Pour ouvrir l'Assistant de récupération dans SafeGuard Management Center, sélectionnez **Outils** > **Récupération** dans la barre de menus.
2. Dans **Type de récupération**, sélectionnez **Clients Sophos SafeGuard** (**autonomes**).
3. Recherchez le fichier de récupération de clé requis en cliquant sur le bouton [**...**] près du champ **Fichier de récupération de clé**. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml.
4. Saisissez le code de challenge que l'utilisateur vous a transmis et cliquez sur **Suivant**. Ce code est vérifié.

   Si le code de challenge a été saisi correctement, l'action de récupération demandée par l'ordinateur, ainsi que les actions de récupération possibles s'affichent. Si le code a été saisi de façon incorrecte, le terme **Challenge non valide** apparaît au-dessous du bloc contenant l'erreur.

5. Sélectionnez l'action que l'utilisateur doit entreprendre, puis cliquez sur **Suivant**.
6. Un code de réponse est généré. Communiquez-le à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L'utilisateur peut saisir le code de réponse, exécuter l'action requise, puis reprendre son travail.

26.3 Récupération du système pour le chiffrement intégral du disque SafeGuard

SafeGuard Enterprise chiffre les fichiers et les lecteurs de façon transparente. Les lecteurs d'initialisation peuvent également être chiffrés et les fonctions de déchiffrement telles que le code, les algorithmes de chiffrement et la clé de chiffrement doivent être disponibles très tôt au cours de la phase d'initialisation. C'est la raison pour laquelle les informations chiffrées ne sont pas accessibles si les modules essentiels de SafeGuard Enterprise ne sont pas disponibles ou ne fonctionnent pas.

Les sections suivantes couvrent les problèmes et les méthodes de récupération envisageables.

26.3.1 Récupération des données via l'initialisation à partir d'un support externe

Ce type de récupération s'applique lorsque l'utilisateur ne peut plus accéder au volume chiffré. Dans ce cas, l'accès aux données chiffrées peut être récupéré en démarrant l'ordinateur à partir d'un disque de récupération Windows PE personnalisé pour SafeGuard Enterprise.

Conditions préalables :

- L'utilisateur qui exécute l'initialisation à partir d'un support externe doit disposer de l'autorisation appropriée. La configuration doit être effectuée dans le BIOS de l'ordinateur.

- L'ordinateur doit prendre en charge l'initialisation à partir de supports autres qu'un disque dur fixe.

Pour récupérer l'accès aux données chiffrées sur l'ordinateur, procédez comme suit :

1. Demandez au support technique de vous fournir le disque SafeGuard Enterprise Windows PE.

   Le support peut télécharger le disque de récupération Windows PE avec les derniers pilotes du filtre Sophos SafeGuard sur le site du support Sophos. Retrouvez plus d'informations dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/108805.aspx.
2. Insérez le disque de récupération Windows PE dans l'ordinateur.
3. Démarrez l'ordinateur à partir du disque de récupération et effectuez une procédure Challenge/Réponse avec un client virtuel. Retrouvez plus d'informations à la section Challenge/Réponse à l'aide de clients virtuels à la page 231.

L'accès aux données stockées sur cette partition est récupéré.

Remarque : en fonction du BIOS en cours d'utilisation, il est possible que l'initialisation depuis le disque ne fonctionne pas.

26.3.2 MBR corrompu

Pour résoudre les problèmes d'enregistrement d'amorçage maître (MBR, Master Boot Record) corrompu, SafeGuard Enterprise propose l'utilitaire **`BE_Restore.exe`**.

Retrouvez une description détaillée de la façon de restaurer un MBR corrompu au moyen de cet utilitaire dans le *Guide des outils de SafeGuard Enterprise.*

26.3.3 Code

Un disque dur dont le code d'initialisation du noyau est endommagé reste accessible car les clés sont stockées séparément du noyau dans la zone de stockage des clés (KSA). En séparant le noyau et les clés, ce type de lecteur peut être déchiffré lorsqu'il est connecté à un autre ordinateur.

Pour ce faire, l'utilisateur qui se connecte à l'autre ordinateur a besoin d'une clé de la KSA pour la partition qui ne peut être initialisée dans son jeu de clés.

Dans le pire des cas, la partition est seulement chiffrée avec le Boot_Key de l'autre ordinateur. Dans une telle situation, le responsable principal de la sécurité ou le responsable récupération doit attribuer ce Boot_Key à l'utilisateur.

Retrouvez plus d'informations à la section Asservissement d'un disque dur à la page 243.

26.3.4 Volumes

SafeGuard Enterprise propose le chiffrement basé sur volume. Cela inclut les informations de chiffrement de l'enregistrement constituées du secteur d'initialisation, de la KSA (KSA, Key Storage Area) principale et de sauvegarde, ainsi que du secteur d'initialisation original sur chaque lecteur.

Si l'une des conditions suivantes s'applique, le volume n'est plus accessible :

- Les deux zones de stockage des clés sont endommagées en même temps.
- Le MBR d'origine est endommagé.

26.3.4.1 Secteur d'initialisation

Au cours du processus de chiffrement, le secteur d'initialisation d'un volume est remplacé par le secteur d'initialisation de SafeGuard Enterprise.

Le secteur d'initialisation de SafeGuard Enterprise contient des informations sur

- L'emplacement de la KSA principale et de sauvegarde dans les clusters et les secteurs en relation au début de la partition
- La taille de la KSA

Même si le secteur d'initialisation de SafeGuard Enterprise est endommagé, les volumes chiffrés sont inaccessibles.

L'utilitaire **`BE_Restore`** peut restaurer le secteur d'initialisation endommagé. Pour plus d'informations, reportez-vous au *Guide d'outils de SafeGuard Enterprise*.

26.3.4.2 Secteur d'initialisation original

Le secteur d'initialisation original est celui qui est exécuté après le déchiffrement de la DEK (Data Encryption Key, clé de chiffrement de données) et après que l'algorithme et la clé ont été chargés dans le pilote du filtre BE.

Si ce secteur d'initialisation est défectueux, Windows n'a pas accès au volume. Normalement le message d'erreur habituel "Le disque n'est pas formaté. Voulez-vous le formater maintenant ? Oui/Non" est affiché.

SafeGuard Enterprise charge néanmoins la DEK pour ce volume. L'outil utilisé pour réparer le secteur d'initialisation doit être compatible avec le filtre de volume supérieur de SafeGuard Enterprise.

26.3.5 Problèmes d'initialisation Windows

Sa conception cryptographique de la clé spécifique du volume (secteur d'initialisation, zone de stockage des clés KSA) confère à SafeGuard Enterprise une très grande souplesse.

Vous pouvez sauver un système endommagé en initialisant un support de restauration à partir de la fonction d'authentification au démarrage SafeGuard (Windows PE avec le sous-système de chiffrement de SafeGuard Enterprise installé). Ces supports ont un accès de chiffrement/déchiffrement transparent aux volumes chiffrés avec SafeGuard Enterprise. Il est possible de remédier ici à la cause du système qui ne peut être initialisé.

26.3.5.1 Sous-système de chiffrement

Les sous-systèmes de chiffrement sont par exemple BEFLT.sys. effectuez la procédure décrite dans Problèmes d'initialisation Windows et réparez le système.

26.3.6 Configuration de WinPE pour SafeGuard Enterprise

Pour accéder aux lecteurs chiffrés avec le BOOTKEY d'un ordinateur dans un environnement WinPE, SafeGuard Enterprise offre WinPE avec les modules de fonction et les pilotes SafeGuard Enterprise. Pour lancer SetupWinPE, entrez la commande suivante :

`SetupWinPE -pe2 <fichier d'image WinPE>`

`fichier d'image WinPE` étant le nom de chemin complet d'un fichier d'image WinPE

SetupWinPE effectue toutes les modifications nécessaires.

Remarque : dans ce type d'environnement WinPE, seuls les lecteurs chiffrés avec le BOOTKEY sont accessibles. Les lecteurs chiffrés avec une clé utilisateur sont inaccessibles car les clés ne sont pas disponibles dans cet environnement.

26.3.7 Asservissement d'un disque dur

SafeGuard Enterprise permet l'asservissement des volumes ou des disques durs chiffrés. Il permet à l'utilisateur final, à l'administrateur Windows et au responsable de la sécurité de SafeGuard Enterprise de se connecter ou de supprimer de nouveaux volumes ou disques durs en dépit du chiffrement basé sur secteur.

La zone de stockage des clés (KSA, Key Storage Area) d'un volume contient toutes les informations nécessaires, c'est-à-dire :

- La DEK (Data Encryption Key, clé de chiffrement des données) générée aléatoirement.
- Un identifiant pour l'algorithme de chiffrement utilisé pour chiffrer le volume.
- La liste des GUID pour les KEK (Key Encryption Keys, clés de chiffrement des clés) qui peuvent chiffrer et déchiffrer la DEK.
- Le volume lui-même contient sa taille.

Un volume chiffré avec SafeGuard Enterprise est accessible à partir de tous les ordinateurs d'extrémité protégés par SafeGuard Enterprise, pourvu que l'utilisateur ou l'ordinateur possède une KEK de la KSA du volume sur son jeu de clés.

Les utilisateurs ou les ordinateurs doivent pouvoir déchiffrer la DEK chiffrée par la KEK.

Un grand nombre d'utilisateurs et d'ordinateurs peuvent accéder à un volume ayant été chiffré avec une KEK distribuable tel qu'une OU, un groupe, ou une clé de domaine, car de nombreux utilisateurs/ordinateurs d'un domaine ont cette clé dans leurs jeux de clés.

Toutefois, un volume qui n'est chiffré qu'avec la clé d'initialisation individuelle ("Boot_nommachine") de l'ordinateur protégé par SafeGuard Enterprise n'est accessible que par cet ordinateur d'extrémité particulier.

Si un volume ne s'initialise pas sur son ordinateur d'origine, il peut être "asservi" sur un autre ordinateur d'extrémité protégé par SafeGuard Enterprise. Toutefois, la clé d'initialisation correcte n'est pas accessible. Elle doit être rendue accessible.

Chaque fois que l'utilisateur tente d'accéder au volume depuis un autre ordinateur, il peut le faire car les KEK de la KSA et le jeu de clés des autres utilisateurs ou ordinateurs correspondent de nouveau.

26.3.7.1 Exemple

Alice possède sa clé utilisateur personnelle. Chaque fois qu'elle est connectée à son autre ordinateur ("Portable_Alice"), elle ne peut pas accéder au volume chiffré avec la clé d'initialisation de l'ordinateur "SGNCLT".

Le "SGMCLT" de l'ordinateur d'extrémité protégé par SafeGuard Enterprise n'a que sa propre clé d'initialisation, BOOT_SGMCLT.

Le responsable de la sécurité attribue la clé d'initialisation "BOOT_SGNCLT" à Alice de la façon suivante :

1. Il sélectionne l'utilisateur Alice.
2. Il clique sur l'icône «Jumelles» dans la barre d'outils de SafeGuard Enterprise. Cela ouvre la boîte de dialogue de recherche qui affiche également les clés d'initialisation.
3. Il sélectionne la clé «BOOT_SGMCLT».

Alice possède désormais deux clés : "Utilisateur_Alice" et "BOOT_SGMCLT". Ceci peut être vérifié dans **Clés et certificats**.

Le "BOOT_SGMCLT" a été attribué deux fois : à l'ordinateur SGMCLT et à l'utilisateur Alice.

Alice peut désormais accéder au volume chiffré de n'importe quel autre ordinateur d'extrémité protégé par SafeGuard Enterprise auquel elle peut se connecter.

Ensuite, elle peut facilement utiliser des outils tels que l'Explorateur Windows ou regedit.exe pour résoudre la cause du problème d'initialisation.

Si, dans le cas le moins favorable, le problème ne peut pas être résolu, elle peut enregistrer les données sur une autre unité, reformater le volume et le reconfigurer entièrement.

27 Restauration d'une installation SafeGuard Management Center en cas de corruption

Si l'installation du SafeGuard Management Center est corrompue mais la base de données est toujours intacte, l'installation peut être restaurée en réinstallant le SafeGuard Management Center et en utilisant la base de données existante ainsi que le certificat sauvegardé du responsable de la sécurité.

- Le certificat du responsable principal de la sécurité de la configuration de la base de données correspondante doit avoir été exporté sous la forme d'un fichier .p12, ainsi qu'être disponible et valide.
- Vous devez également connaître les mots de passe de ce fichier .p12, ainsi que ceux du magasin de certificats.

Pour restaurer l'installation corrompue du SafeGuard Management Center :

1. Réinstallez le package d'installation du SafeGuard Management Center. Ouvrez le SafeGuard Management Center. L'assistant de configuration démarre automatiquement.
2. Dans **Connexion à la base de données**, sélectionnez le serveur de base de données correspondant et configurez la connexion à la base de données, le cas échéant. Cliquez sur **Suivant**.
3. Dans **Paramètres de base de données**, cliquez sur **Sélectionner une base de données disponible** et sélectionnez dans la liste la base de données correspondante.
4. Dans **Responsable de la sécurité**, exécutez l'une des actions suivantes :
   - Si le fichier de certificat sauvegardé se trouve sur l'ordinateur, il s'affiche. Saisissez le mot de passe que vous utilisez pour vous authentifier dans le SafeGuard Management Center.
   - Si le fichier de certificat sauvegardé est introuvable sur l'ordinateur, cliquez sur **Importer**. Recherchez le fichier de certificat sauvegardé et cliquez sur **Ouvrir**. Saisissez le mot de passe du fichier de certificat sélectionné. Cliquez sur **Oui**. Saisissez et confirmez le mot de passe d'authentification dans le SafeGuard Management Center.
5. Cliquez sur **Suivant**, puis sur **Terminer** pour achever la configuration du SafeGuard Management Center.

L'installation corrompue du SafeGuard Management Center est restaurée.

28 Restauration d'une configuration de base de données corrompue

La configuration corrompue d'une base de données peut être restaurée en réinstallant le SafeGuard Management Center pour créer une nouvelle instance de la base de données, d'après les fichiers de certificat sauvegardés. Vous garantissez ainsi que tous les ordinateurs d'extrémité SafeGuard Enterprise existants acceptent les stratégies de la nouvelle installation.

- Les certificats d'entreprise et du responsable principal de la sécurité pour la configuration de la base de données correspondante doivent avoir été exportés sous la forme de fichiers .p12, ainsi qu'être disponibles et valides.
- Vous devez également connaître les mots de passe de ces deux fichiers .p12, ainsi que du magasin de certificats.

Remarque : nous conseillons seulement ce type de restauration si aucune sauvegarde de base de données valide n'est disponible. Tous les ordinateurs connectés à un client qui a été restauré de cette façon perdront leur attribution utilisateur/machine. L'authentification au démarrage SafeGuard sera provisoirement désactivée. Les mécanismes de challenge/réponse ne seront pas disponibles tant que l'ordinateur d'extrémité correspondant n'aura pas renvoyé avec succès les informations sur sa clé.

Pour restaurer une configuration de base de données corrompue :

1. Réinstallez le package d'installation du SafeGuard Management Center. Ouvrez le SafeGuard Management Center. L'**Assistant de configuration** démarre automatiquement.
2. Dans **Connexion à la base de données**, cochez la case **Créer une base de données**. Sous **Paramètres de base de données**, configurez la connexion à la base de données. Cliquez sur **Suivant**.
3. Dans **Données du responsable de la sécurité**, sélectionnez le responsable principal de la sécurité correspondant, puis cliquez sur **Importer**.
4. Cliquez sur **Importer le certificat d'authentification** pour rechercher le fichier de certificat sauvegardé. Sous **Fichier de certificat logiciel**, entrez le mot de passe de ce fichier. Cliquez sur **OK**.
5. Le certificat du responsable principal de la sécurité est alors importé. Cliquez sur **Suivant**.
6. Dans **Certificat d'entreprise**, cochez la case **Restaurer à l'aide d'un certificat d'entreprise existant.** Cliquez sur **Importer** pour rechercher le fichier de certificat sauvegardé qui contient le certificat d'entreprise valide. Vous êtes invité à saisir le mot de passe défini pour le magasin de certificats. Saisissez le mot de passe et cliquez sur **OK** pour le confirmer. Cliquez sur **Oui** dans le message affiché.

   Le certificat d'entreprise est alors importé.
7. Cliquez sur **Suivant**, puis sur **Terminer**.

La configuration de la base de données est restaurée.

29 Données d'inventaire et d'état

SafeGuard Enterprise lit une quantité considérable de données d'inventaire et d'état provenant des ordinateurs d'extrémité. Ces données indiquent l'état général en cours de chaque ordinateur. Ces données s'affichent clairement dans le SafeGuard Management Center, dans **Utilisateurs et ordinateurs** dans l'onglet **Inventaire**.

En tant que responsable de la sécurité, vous pouvez afficher, exporter et imprimer les données d'inventaire et d'état. Par exemple, vous pouvez créer des rapports de conformité pour prouver que des ordinateurs d'extrémité ont été chiffrés. Les fonctions de tri et de filtrage étendus sont disponibles pour vous aider à sélectionner les données pertinentes.

L'**inventaire** propose, par exemple, les données suivantes sur chaque machine :

- La stratégie appliquée.
- Le dernier contact du serveur.
- L'état de chiffrement de tous les supports.
- L'état et le type de l'authentification au démarrage.
- Les modules SafeGuard Enterprise installés.
- L'état de l'éveil par appel réseau sécurisé (WOL).
- Les données utilisateur.

29.1 Ordinateurs d'extrémité Mac dans l'inventaire

L'**Inventaire** permet d'obtenir des données d'état pour les Macs administrés dans SafeGuard Management Center. Retrouvez plus d'informations à la section Données d'inventaire et d'état des Mac à la page 277

29.2 Affichage des données d'inventaire

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation, cliquez sur le conteneur concerné (domaine, groupe de travail ou ordinateur) à gauche.
3. Dans la zone d'action, accédez à l'onglet **Inventaire** à droite.
4. Dans la zone **Filtre**, sélectionnez le filtre à appliquer à l'écran d'inventaire. Retrouvez plus d'informations à la section Filtrage des données d'inventaire à la page 248.

   Remarque : si vous sélectionnez un ordinateur particulier, les données d'inventaire sont reçues dès que vous accédez à l'onglet **Inventaire**. La zone **Filtre** n'est pas disponible ici.

5. Dans la zone **Filtre**, cliquez sur la loupe.

Les données d'inventaire et d'état s'affichent sous forme de tableau récapitulatif de toutes les machines du conteneur sélectionné. Les onglets **Lecteurs**, **Utilisateurs** et **Fonctions** sont également disponibles pour chaque machine.

Cliquez sur l'en-tête de la colonne pour trier les données d'inventaire par les valeurs de la colonne sélectionnée. Le menu contextuel de chaque colonne propose de nombreuses fonctions de tri, de regroupement et de personnalisation de l'affichage. En fonction de vos droits d'accès, les éléments dans l'inventaire apparaissent dans des couleurs différentes :

- Les éléments des objets pour lesquels vous avez des droits d'**Accès complet** apparaissent en noir.
- Les éléments des objets pour lesquels vous avez des droits d'accès en **Lecture seule** apparaissent en bleu.
- Les éléments des objets pour lesquels vous n'avez aucun droit d'accès sont grisés.

29.3 Affichage des colonnes masquées

Dans l'affichage des données d'inventaire, certaines colonnes sont masquées par défaut.

1. Dans cet affichage, cliquez avec le bouton droit de la souris sur la barre d'en-têtes de colonnes.
2. Dans le menu contextuel, sélectionnez **Exécuter la personnalisation de colonne**.

   La fenêtre **Personnalisation** apparaît affichant les colonnes cachées.

3. Déplacez la colonne requise depuis la fenêtre **Personnalisation** vers la barre d'en-têtes de colonnes.

La colonne apparaît dans l'affichage des données d'inventaire Pour la masquer de nouveau, déplacez-la de nouveau dans la fenêtre **Personnalisation**.

29.4 Filtrage des données d'inventaire

Lorsque vous utilisez une OU, des filtres peuvent être définis pour limiter l'affichage en fonction d'un critère particulier.

Les champs suivants sont disponibles pour définir des filtres dans la zone **Filtre** de l'onglet **Inventaire** :

Champ	Description
Nom de l'ordinateur	Pour afficher les données d'inventaire et d'état d'un ordinateur particulier, entrez le nom de l'ordinateur dans ce champ.
Sous-conteneurs inclus	Activez ce champ pour inclure les sous-conteneurs à l'écran.
Afficher dernier modifié	Utilisez ce champ pour spécifier le nombre de dernières modifications à afficher.

Vous pouvez également utiliser l'éditeur de filtres pour créer des filtres définis par l'utilisateur. Vous pouvez ouvrir l'éditeur de filtres depuis le menu contextuel de chaque colonne. Dans la fenêtre **Générateur de filtres**, vous pouvez définir des filtres personnalisés et les appliquer à la colonne concernée.

29.5 Actualisation des données d'inventaire

Les ordinateurs d'extrémité envoient et mettent généralement à jour les données d'inventaire lorsqu'elles sont modifiées.

La commande **Demander une actualisation de l'inventaire** peut être utilisée pour demander manuellement une actualisation des données d'inventaire actuelles de l'ordinateur. Cette commande est disponible pour un ordinateur particulier ou pour tous les ordinateurs d'un nœud (pouvant inclure des nœuds secondaires) depuis le menu contextuel et le menu **Actions** de la barre de menus SafeGuard Management Center. La commande peut également être sélectionnée via le menu contextuel des entrées de la liste.

Si vous sélectionnez cette commande ou cliquez sur l'icône **Demander une actualisation de l'inventaire** dans la barre d'outils, les ordinateurs concernés envoient leurs données d'inventaire actuelles.

Comme cela est le cas avec d'autres zones du SafeGuard Management Center, vous pouvez utiliser la commande **Actualiser** pour actualiser l'affichage. Vous pouvez sélectionner cette commande dans le menu contextuel pour les ordinateurs individuels ou tous les ordinateurs d'un nœud et dans le menu **Afficher** de la barre de menus. Vous pouvez également utiliser l'icône à double flèche **Actualiser** dans la barre d'outils pour actualiser l'affichage.

29.6 Présentation

Les colonnes individuelles dans la présentation proposent les informations suivantes :

Remarque : certains colonnes sont cachées par défaut. Vous pouvez personnaliser l'affichage pour les montrer. Retrouvez plus d'informations à la section Affichage des colonnes cachées à la page 248.

Colonne	Explication
Nom de la machine	Indique le nom de l'ordinateur.
Domaine	Indique le nom du domaine de l'ordinateur.
Domaine Pre 2000	Indique le nom du domaine avant Windows 2000.
Nom utilisateur (propriétaire)	Indique le nom utilisateur du propriétaire de l'ordinateur, s'il est disponible.
Prénom	Indique le prénom du propriétaire, s'il est disponible.
Nom	Indique le nom de famille du propriétaire, s'il est disponible.
Adresse électronique	Indique l'adresse électronique du propriétaire, s'il est disponible.

Colonne	Explication
Autres utilisateurs enregistrés	Affiche les noms des autres utilisateurs enregistrés de l'ordinateur, s'ils sont disponibles.
Système d'exploitation	Indique le système d'exploitation de l'ordinateur.
Dernier contact du serveur	Indique la date et l'heure auxquelles l'ordinateur a communiqué avec le serveur pour la dernière fois.
Dernière stratégie reçue	Indique la date et l'heure auxquelles l'ordinateur a reçu la dernière stratégie.
Lecteurs chiffrés	Indique les lecteurs chiffrés de l'ordinateur.
Lecteurs non chiffrés	Indique les lecteurs non chiffrés de l'ordinateur.
Type de chiffrement	Indique si l'ordinateur est un ordinateur d'extrémité SafeGuard Enterprise natif, un ordinateur d'extrémité BitLocker avec Challenge/Réponse SafeGuard, un ordinateur d'extrémité BitLocker avec mécanisme de récupération natif, un ordinateur d'extrémité FileVault 2 ou un ordinateur d'extrémité avec un lecteur de disque dur conforme à la norme d'auto-chiffrement Opal.
Authentification au démarrage (POA)	Indique si l'authentification au démarrage SafeGuard est activée pour l'ordinateur.
Éveil par appel réseau	Spécifie si l'éveil par appel réseau est activé pour l'ordinateur.
Date de modification	Indique la date à laquelle les données d'inventaire ont changé en raison d'une demande d'actualisation de l'inventaire ou de l'envoi de l'ordinateur de nouvelles données d'inventaire.
Actualisation demandée	Indique la date de la dernière demande d'actualisation. La valeur affichée dans ce champ sera supprimée une fois la demande traitée par l'ordinateur.
DSN parent	Indique le nom distinctif de l'objet conteneur auquel l'ordinateur est subordonné. Cette colonne ne s'affiche que si le champ **Sous-conteneurs inclus** a été activé dans la zone **Filtre**.
Certificat d'entreprise actuel	Indique si l'ordinateur utilise le certificat d'entreprise actuel.

29.7 Onglet Lecteurs

L'onglet **Lecteurs** indique les données d'inventaire et d'état des lecteurs sur l'ordinateur concerné.

Colonne	Explication
Nom du lecteur	Indique le nom du lecteur.
Étiquette	Identifie un lecteur Mac

Colonne	Explication
Type	Indique le type de lecteur, par exemple **Fixe**, **Support amovible** ou **CD-ROM/DVD**.
État	Indique l'état de chiffrement d'un lecteur. **Remarque :** si la gestion de SafeGuard BitLocker est installée sur un ordinateur d'extrémité, il se peut que l'état de chiffrement d'un lecteur indique **Non préparé**. Ceci signifie que le lecteur ne peut actuellement pas être chiffré avec BitLocker car les préparations d'usage n'ont pas encore été effectuées. Ceci s'applique uniquement aux ordinateurs d'extrémité administrés. En effet, les ordinateurs d'extrémité non administrés ne sont pas en mesure de créer des rapports sur les données d'inventaire. Retrouvez plus d'informations sur les conditions préalables requises pour gérer et chiffrer les lecteurs BitLocker à la section Conditions préalables à la gestion de BitLocker sur les ordinateurs d'extrémité à la page 155. L'état de chiffrement d'un ordinateur d'extrémité non administré peut être vérifié à l'aide de l'outil de ligne de commande SGNState. Retrouvez plus d'informations dans le *Guide des outils de SafeGuard Enterprise*.
Algorithme	Pour les lecteurs chiffrés, ce champ indique l'algorithme utilisé pour le chiffrement.

29.8 Onglet Utilisateurs

L'onglet **Utilisateurs** indique les données d'inventaire et d'état des utilisateurs sur l'ordinateur.

Colonne	Explication
Nom d'utilisateur	Indique le nom de l'utilisateur.
Nom distinctif	Indique le nom DNS de l'utilisateur, par exemple : CN=Administrateur,CN=Utilisateurs,DC=domaine,DC=monentreprise,DC=net
Utilisateur propriétaire	Indique si l'utilisateur est défini comme étant le propriétaire de l'ordinateur.
Utilisateur verrouillé	Indique si l'utilisateur est verrouillé.
Utilisateur Windows de SGN	Indique si l'utilisateur est un utilisateur Windows de SGN. Un utilisateur Windows de SGN n'est pas ajouté à l'authentification au démarrage SafeGuard. En revanche, il dispose d'un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur Sophos SGN. Vous pouvez activer l'enregistrement des utilisateurs Windows de SGN sur les ordinateurs d'extrémité grâce à des stratégies de type **Paramètres de machine spécifiques**.

29.9 Onglet Fonctions

L'onglet **Fonctions** propose une présentation de tous les modules SafeGuard Enterprise installés sur l'ordinateur.

Colonne	Explication
Nom du module	Indique le nom du module SafeGuard Enterprise installé.
Version	Indique la version logicielle du module SafeGuard Enterprise installé.

29.10 Onglet Certificat d'entreprise

L'onglet **Certificat d'entreprise** affiche les propriétés du certificat d'entreprise actuellement utilisé et indique si un certificat plus récent est disponible.

Colonne	Explication
Sujet	Affiche le nom distinctif du sujet du certificat d'entreprise.
Serial	Affiche le numéro de série du certificat d'entreprise.
Émetteur	Affiche le nom distinctif de l'émetteur du certificat d'entreprise.
Valide à compter du	Affiche la date et l'heure du début de la validité du certificat d'entreprise.
Valide jusqu'au	Affiche la date et l'heure de l'expiration du certificat d'entreprise.
Un certificat d'entreprise plus récent est disponible	Indique si un certificat d'entreprise plus récent que l'actuel de l'ordinateur d'extrémité est disponible.

29.11 Création de rapports des données d'inventaire

En tant que responsable de la sécurité, vous pouvez créer des rapports des données d'inventaire dans différents formats. Par exemple, vous pouvez créer des rapports de conformité pour prouver que des ordinateurs d'extrémité ont été chiffrés. Les rapports peuvent être imprimés ou exportés dans un fichier.

29.11.1 Impression de rapports d'inventaire

1. Dans la barre de menus du SafeGuard Management Center, cliquez sur **Fichier**.
2. Vous pouvez soit imprimer le rapport directement, soit afficher un aperçu avant impression.

L'aperçu avant impression fournit plusieurs fonctions, par exemple pour la modification de la mise en page (en-tête et pied de page, etc.).

- Pour obtenir un aperçu avant impression, sélectionnez **Imprimer** > **Aperçu**.
- Pour imprimer le document sans afficher l'aperçu, sélectionnez **Imprimer**.

29.11.2 Exportation des rapports d'inventaire dans les fichiers

1. Dans la barre de menus du SafeGuard Management Center, cliquez sur **Fichier**.
2. Sélectionnez **Imprimer** > **Aperçu**.

   Le rapport d'inventaire **Aperçu** apparaît.

   L'aperçu fournit plusieurs fonctions, par exemple pour la modification de la mise en page (en-tête et pied de page, etc.).

3. Dans la barre d'outils de la fenêtre **Aperçu**, sélectionnez la liste déroulante de l'icône **Exporter le document...**.
4. Dans la liste, sélectionnez le type de fichier requis.
5. Indiquez les options d'exportation nécessaires et cliquez sur **OK**.

Le rapport d'inventaire est exporté dans un fichier du type spécifié.

30 Rapports

La possibilité de signaler des incidents liés à la sécurité est une condition préalable à une analyse détaillée du système. Les événements journalisés facilitent le suivi exact des processus sur une station de travail donnée ou dans un réseau. En journalisant les événements, vous pouvez par exemple vérifier les atteintes à la sécurité commises par de tiers. A l'aide des fonctionnalités de journalisation, les administrateurs et responsables de la sécurité peuvent aussi détecter les erreurs dans l'affectation de droits utilisateur et les corriger.

SafeGuard Enterprise journalise toutes les activités et informations de l'état de l'ordinateur d'extrémité, ainsi que les actions de l'administrateur et les événements liés à la sécurité, puis les enregistre de manière centralisée. Les fonctionnalités de journalisation enregistrent les événements déclenchés par les produits SafeGuard installés. Le type de journaux est défini dans les stratégies du type **Journalisation**. C'est aussi où vous spécifiez le résultat et l'emplacement de sauvegarde des événements journalisés : le journal des événements Windows de l'ordinateur d'extrémité ou la base de données SafeGuard Enterprise.

En tant que responsable de la sécurité disposant des droits nécessaires, vous pouvez afficher, imprimer et archiver les informations d'état et les rapports de journaux affichés dans le SafeGuard Management Center. Le SafeGuard Management Center propose des fonctions de tri et de filtrage complètes très utiles lors de la sélection d'événements pertinents à partir des informations disponibles.

Des analyses automatiques de la base de données de journaux, par exemple avec Crystal Reports ou Microsoft System Center Operations Manager, sont également possibles. SafeGuard Enterprise protège les entrées des journaux contre toute manipulation non autorisée à l'aide de signatures sur le client et sur le serveur.

En fonction de la stratégie de journalisation, les événements des catégories suivantes peuvent être journalisés :

- Authentification
- Administration
- Système
- Chiffrement
- Client
- Contrôle d'accès

Pour SafeGuard Data Exchange, vous pouvez avoir un suivi des fichiers accédés sur les supports amovibles en journalisant les événements correspondants. Retrouvez plus d'informations sur ce type de rapport à la section Rapport d'accès aux fichiers pour les supports amovibles à la page 259.

30.1 Scénarios d'application

Les fonctionnalités de journalisation de SafeGuard Enterprise constituent une solution conviviale et complète pour l'enregistrement et l'analyse des événements. Les exemples suivants illustrent des scénarios d'application types des **Rapports** de SafeGuard Enterprise.

30.1.1 Contrôle centralisé des ordinateurs d'extrémité d'un réseau

Le responsable de la sécurité souhaite être régulièrement informé des événements critiques (accès non autorisé aux données, nombre d'échecs de tentatives de connexion sur une période spécifiée, par exemple). Grâce à une stratégie de journalisation, le responsable de la sécurité peut configurer la journalisation dans un fichier journal local de processus afin de journaliser tous les événements liés à la sécurité survenus sur les ordinateurs d'extrémité. Ce fichier journal est transféré dans la base de données SafeGuard Enterprise via le serveur SafeGuard Enterprise une fois atteint un certain nombre d'événements. Le responsable de la sécurité peut récupérer, afficher et analyser les événements dans la **Observateur d'événements** du SafeGuard Management Center. Les processus exécutés sur différents ordinateurs d'extrémité peuvent ainsi être audités sans intervention du personnel sur la journalisation.

30.1.2 Surveillance des utilisateurs mobiles

Les utilisateurs mobiles ne sont généralement pas connectés en permanence au réseau de l'entreprise. Par exemple, les commerciaux déconnectent leur portable pendant une réunion. Dès qu'ils se reconnectent au réseau, les événements SafeGuard Enterprise journalisés pendant la période hors ligne sont transférés. Les fonctionnalités de journalisation proposent une vue d'ensemble précise des activités de l'utilisateur pendant la période de déconnexion de l'ordinateur.

30.2 Condition préalable

Les événements sont gérés par le serveur SafeGuard Enterprise. Sur un ordinateur sur lequel se trouve uniquement SafeGuard Management Center, assurez-vous que les événements sont envoyés au serveur SafeGuard Enterprise. Veuillez donc installer un package de configuration client sur l'ordinateur du SafeGuard Management Center indiquant à ce dernier où est placé le serveur SafeGuard Enterprise. Ainsi, l'ordinateur est activé en tant que client sur le serveur et les fonctionnalités de journalisation Windows ou SafeGuard Enterprise sont activées.

Retrouvez plus d'informations sur les packages de configuration client à la section Utilisation des packages de configuration à la page 83.

30.3 Destinations des événements journalisés

Il y a deux destinations possibles pour les événements journalisés : l'Observateur d'événements Windows ou la base de données SafeGuard Enterprise. Seuls les événements liés à un produit SafeGuard sont inscrits à la destination correspondante.

Les destinations de sortie des événements à journaliser sont spécifiées dans la stratégie de journalisation.

30.3.1 Observateur d'événements Windows

Les événements pour lesquels vous définissez l'Observateur d'événements Windows comme destination dans la stratégie de journalisation sont journalisés dans l'Observateur d'événements Windows. L'Observateur d'événements Windows peut être utilisée pour afficher et gérer les journaux des événements liés au système, à la sécurité et à l'application. Vous pouvez également enregistrer ces journaux d'événements. Un compte administrateur sur l'ordinateur d'extrémité concerné est requis pour ces procédures. Dans l'Observateur d'événements Windows, un code d'erreur s'affiche à la place d'un texte descriptif de l'événement.

Remarque : une condition préalable à l'affichage des événements SafeGuard Enterprise dans l'Observateur d'événements Windows consiste à avoir installé un package de configuration client sur l'ordinateur d'extrémité.

Remarque : ce chapitre décrit les processus d'affichage, de gestion et d'analyse des journaux d'événements dans le SafeGuard Management Center. Retrouvez plus d'informations sur l'Observateur d'événements Windows dans votre documentation Microsoft.

30.3.2 Base de données SafeGuard Enterprise

Les événements pour lesquels vous définissez la base de données SafeGuard Enterprise comme destination dans la stratégie de journalisation sont collectés dans un fichier journal local dans le cache local de l'ordinateur d'extrémité concerné dans le répertoire suivant : auditing\SGMTranslog. Les fichiers journaux sont soumis à un mécanisme de transport qui les transfère dans la base de données via le serveur SafeGuard Enterprise. Par défaut, le fichier est soumis dès que le mécanisme de transport a établi une connexion avec le serveur. Pour limiter la taille d'un fichier journal, vous pouvez définir un nombre maximal d'entrées du journal dans une stratégie du type **Paramètres généraux**. Le fichier journal est soumis dans la file d'attente de transport du serveur SafeGuard Enterprise une fois le nombre d'entrées spécifié atteint. Les événements journalisés dans la base de données centrale peuvent être affichés dans l'**Observateur d'événements** ou dans le **Visualiseur de suivi des fichiers** de SafeGuard Enterprise. En tant que responsable de la sécurité, vous devez disposer des droits appropriés pour afficher, analyser et gérer les événements journalisés dans la base de données.

30.4 Configuration des paramètres de journalisation

Les paramètres de rapport sont définis à l'aide de deux stratégies :

- Stratégie **Paramètres généraux**

  Dans une stratégie **Paramètres généraux**, vous pouvez spécifier un nombre maximum d'entrées journalisées au-delà duquel le fichier journal contenant les événements destinés à la base de données centrale doit être transféré dans la base de données de SafeGuard Enterprise. Ceci permet de réduire la taille des fichiers journaux individuels à transférer. Ce paramètre est facultatif.

- Stratégie **Journalisation**

Les événements à journaliser sont spécifiés dans une stratégie de journalisation. Dans cette stratégie, un responsable de la sécurité avec les droits de stratégie requis définit quels événements seront journalisés et dans quelle destination en sortie.

30.4.1 Définition du nombre d'événements pour commentaires

1. Cliquez sur **Rapports** dans le SafeGuard Management Center.
2. Créez une stratégie **Paramètres généraux** ou sélectionnez une stratégie existante.
3. Sous **Journalisation**, dans le champ **Commentaires après un certain nombre d'événements**, spécifiez le nombre maximum d'événements pour un fichier journal.
4. Enregistrez vos paramètres.

Après l'attribution de la stratégie, le nombre d'événements spécifié s'applique.

30.4.2 Sélection des événements

1. Dans SafeGuard Management Center, sélectionnez les **Stratégies**.
2. Créez une nouvelle stratégie **Journalisation** ou sélectionnez une stratégie existante.

   Dans la zone d'action de droite,sous **Journalisation**, tous les événements prédéfinis qui peuvent être journalisés apparaissent. Par défaut, les événements sont regroupés par **Niveau**, par exemple **Avertissement** ou **Erreur**. Vous avez la possibilité de changer la manière de les regrouper. Cliquez sur les en-têtes de colonnes pour trier les événements par **ID**, **Catégorie**, etc.

3. Pour indiquer qu'un événement doit être journalisé dans la base de données SafeGuard Enterprise, sélectionnez l'événement en cliquant sur la colonne contenant l'icône de base de données **Consigner les événements dans une base de données**. Pour les événements à journaliser dans l'Observateur d'événements Windows, cliquez dans la colonne contenant l'icône du journal des événements **Consigner dans le journal des événements**.

   Cliquez plusieurs fois pour dessélectionner l'événement ou le rendre nul. Si vous ne définissez pas de paramètre pour un événement, la valeur par défaut correspondante s'applique.

4. Pour tous les événements sélectionnés, une coche verte s'affiche dans la colonne correspondante. Enregistrez vos paramètres.

Après avoir attribué la stratégie, les événements sélectionnés sont journalisés dans la destination en sortie correspondante.

Remarque : retrouvez une liste de tous les événements pouvant être journalisés à la section Événements disponibles pour les rapports à la page 282.

30.5 Visualisation des événements journalisés

En tant que responsable de la sécurité disposant des droits nécessaires, vous pouvez visualiser les événements journalisés dans la base de données centrale de l'**Observateur d'événements** du SafeGuard Management Center.

Pour récupérer les entrées journalisées dans la base de données centrale :

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la zone de navigation **Rapports**, sélectionnez **Observateur d'événements**.
3. Dans la zone d'action **Observateur d'événements** à droite, cliquez sur l'icône de la loupe.

Tous les événements journalisés dans la base de données centrale apparaissent dans l'**Observateur d'événements**.

Les colonnes indiquent les informations suivantes relatives aux événements journalisés :

Colonne	Description
Identifiant	Affiche un numéro identifiant l'événement.
Événement	Affiche un texte d'événement (description de l'événement).
Catégorie	Classification de l'événement selon la source (Chiffrement, Authentification, Système, par exemple).
Application	Affiche la zone logicielle d'où l'événement provient (SGMAuth, SGBaseENc, SGMAS, par exemple).
Ordinateur	Affiche le nom de l'ordinateur sur lequel l'événement journalisé s'est produit.
Domaine de l'ordinateur	Affiche le domaine de l'ordinateur sur lequel l'événement journalisé s'est produit.
Utilisateur	Affiche l'utilisateur connecté lorsque l'événement s'est produit.
Domaine utilisateur	Affiche le domaine de l'utilisateur connecté lorsque l'événement s'est produit.
Heure de connexion	Affiche la date et l'heure système auxquelles l'événement a été journalisé sur l'ordinateur d'extrémité.

Cliquez sur les en-têtes de colonnes pour trier les événements par **Niveau**, **Catégorie**, etc.

Le menu contextuel des colonnes propose également de nombreuses fonctions de tri, de regroupement et de personnalisation de la Visionneuse des événements.

Cliquez deux fois sur une entrée de l'**Observateur d'événements** pour afficher des détails sur l'événement journalisé.

30.5.1 Application de filtres dans l'Observateur d'événements SafeGuard Enterprise

Le SafeGuard Management Center propose des fonctions de filtrage complètes. Grâce à ces fonctions, vous pouvez récupérer rapidement les événements appropriés parmi ceux affichés.

La zone **Filtre** de l'**Observateur d'événements** offre les champs suivants pour la définition des filtres :

Champ	Description
Catégories	Grâce à ce champ, vous pouvez filtrer la **Observateur d'événements** en fonction de la classification source (par exemple **Chiffrement**, **Authentification**, **Système**) affichée dans la colonne **Catégorie**. Sélectionnez les catégories souhaitées dans la liste déroulante du champ.
Niveau d'erreur	Grâce à ce champ, vous pouvez filtrer la **Observateur d'événements** en fonction de la classification des événements Windows (par exemple, avertissement, erreur) indiquée dans la colonne **Niveau**. Sélectionnez les niveaux souhaités dans la liste déroulante du champ.
Afficher dernier	Dans ce champ, vous pouvez définir le nombre d'événements à afficher. Les derniers événements journalisés sont affichés (par défaut, les 100 derniers événements).

Vous pouvez également créer des filtres personnalisés à l'aide de l'éditeur de filtres. Vous pouvez afficher l'éditeur de filtres dans le menu contextuel des colonnes d'un rapport. Dans la fenêtre **Générateur de filtres**, vous pouvez définir des filtres et les appliquer à la colonne concernée.

30.6 Rapport d'accès aux fichiers pour les supports amovibles

Pour SafeGuard Data Exchange, vous pouvez avoir un suivi des fichiers accédés sur les supports amovibles. Quelle que soit la stratégie de chiffrement s'appliquant aux fichiers stockés sur les supports amovibles, les événements peuvent être consignés pour ce qui suit :

- Un fichier ou répertoire est créé sur un périphérique amovible.
- Un fichier ou répertoire est renommé sur un périphérique amovible.
- Un fichier ou répertoire est supprimé d'un périphérique amovible.

Les événements de suivi d'accès aux fichiers peuvent être visualisés dans l'Observateur d'événements Windows ou dans l'**Observateur de suivi des fichiers** de SafeGuard Enterprise en fonction de la destination que vous spécifiez lorsque vous définissez la stratégie de journalisation.

30.6.1 Configuration du suivi d'accès aux fichiers pour les supports amovibles

1. Dans le SafeGuard Management Center, sélectionnez **Stratégies**.
2. Créez une nouvelle stratégie **Journalisation** ou sélectionnez une stratégie existante.

   Dans la zone d'action de droite,sous **Journalisation**, tous les événements prédéfinis qui peuvent être journalisés apparaissent. Cliquez sur les en-têtes de colonnes pour trier les événements par **ID**, **Catégorie**, etc.

3. Pour activer le suivi d'accès aux fichiers stockés sur les supports amovibles, sélectionnez les événements de journalisation suivants en fonction de vos besoins :
   - ID 3020 File tracking CREATE
   - ID 3021 File tracking RENAME
   - ID 3022 File tracking DELETE

   Pour spécifier qu'un événement doit être journalisé dans la base de données SafeGuard Enterprise, sélectionnez l'événement en cliquant sur la colonne contenant l'icône de base de données **Consigner les événements dans une base de données**. Pour les événements à journaliser dans l'Observateur d'événements Windows, cliquez dans la colonne contenant l'icône du journal des événements **Consigner dans le journal des événements**.

   Pour tous les événements sélectionnés, une coche verte s'affiche dans la colonne correspondante.
4. Enregistrez vos paramètres.

Après attribution de la stratégie, le suivi d'accès aux fichiers sur les supports amovibles est activé et les événements sélectionnés sont journalisés dans la destination en sortie correspondante.

30.6.2 Affichage des événements de suivi d'accès aux fichiers

Pour afficher les journaux de suivi d'accès aux fichiers, vous avez besoin du droit **Afficher les événements de suivi des fichiers**.

1. Dans la zone de navigation du SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la zone de navigation **Rapports**, sélectionnez **Observateur de suivi des fichiers**.
3. Dans la zone d'action **Observateur de suivi des fichiers** à droite, cliquez sur la loupe.

Tous les événements journalisés dans la base de données centrale apparaissent dans le **Observateur de suivi des fichiers**. L'affichage est identique à celui de l'**Observateur d'événements**. Retrouvez plus d'informations à la section Visualisation des événements journalisés à la page 257.

30.7 Impression de rapports

Vous pouvez imprimer les rapports d'événements affichés dans l'a **Observateur d'événements** ou de l'**Observateur de suivi des fichiers** du SafeGuard Management Center à partir du menu **Fichier** dans la barre de menus du SafeGuard Management Center.

- Pour afficher un aperçu avant l'impression du rapport, sélectionnez **Fichier** > **Aperçu avant impression.** L'aperçu avant impression propose différentes fonctions comme l'exportation du document dans divers formats de sortie (par exemple, PDF) ou la modification de la mise en page (par exemple, en-tête et pied de page).
- Pour imprimer le document sans afficher l'aperçu, sélectionnez **Fichier** > **Imprimer**.

30.8 Connexion des événements journalisés

Les événements destinés à la base de données centrale sont journalisés dans le tableau EVENT de la base de données de SafeGuard Enterprise. Une protection d'intégrité spécifique peut être appliquée à ce tableau. Les événements peuvent être journalisés sous forme de liste connectée dans le tableau EVENT. En raison de la connexion, chaque entrée de la liste dépend de l'entrée précédente. Si une entrée est supprimée de la liste, ceci apparaît clairement et peut être vérifié à l'aide d'une vérification de l'intégrité.

Pour optimiser les performances, la connexion des événements dans le tableau EVENT est désactivée par défaut. Vous pouvez activer la connexion des événements journalisés pour vérifier l'intégrité. Retrouvez plus d'informations à la section Vérification de l'intégrité des événements journalisés à la page 261.

Remarque : la protection d'intégrité ne s'applique pas au tableau EVENT lorsque la connexion des événements journalisés est désactivée.

Remarque : un trop grand nombre d'événements peut entraîner des problèmes de performances. Retrouvez plus d'informations sur la manière d'éviter ces problèmes de performances lors du nettoyage des événements à la section Nettoyage d'événement planifié par script à la page 263.

30.8.1 Activation de la connexion des événements journalisés

1. Arrêtez le service Web SGNSRV sur le serveur Web.
2. Supprimez tous les événements de la base de données et créez une sauvegarde lors de la suppression. Retrouvez plus d'informations à la section Suppression de tous les événements ou d'une sélection d'événements à la page 262.

   Remarque : si vous ne supprimez pas tous les anciens événements de la base de données, la connexion ne fonctionnera pas correctement car elle n'était pas activée pour les anciens événements restants.

3. Définissez la clé de registre suivante sur 0 ou supprimez-la :

   HKEY_LOCAL_MACHINE\SOFTWARE\Utimaco\SafeGuard Enterprise DWORD : DisableLogEventChaining = 0

4. Redémarrez le service Web.

La connexion des événements journalisés est activée.

Remarque : pour désactiver de nouveau la connexion des événements, définissez la clé de registre sur 1.

30.9 Vérification de l'intégrité des événements journalisés

Condition préalable : Pour vérifier l'intégrité des événements journalisés, la concaténation des événements dans le tableau EVENT doit être activée.

1. Dans le SafeGuard Management Center, cliquez sur **Rapports**.

2. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Actions** > **Vérifier l'intégrité**.

Un message affiche des informations sur l'intégrité des événements journalisés.

Remarque : si la connexion des événements est désactivée, une erreur est renvoyée.

30.10 Suppression de tous les événements ou d'une sélection d'événements

1. Dans le SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans l'**Observateur d'événements**, sélectionnez les événements à supprimer.
3. Pour supprimer des événements sélectionnés, sélectionnez **Actions** > **Supprimer des événements** ou cliquez sur l'**Icône de suppression des événements** dans la barre d'outils. Pour supprimer tous les événements, sélectionnez **Actions** > **Supprimer tous les événements** ou cliquez sur l'**Icône de suppression de tous les événements** dans la barre d'outils.
4. Avant de supprimer les événements sélectionnés, le système affiche la fenêtre **Sauvegarder les événements sous** permettant de créer un fichier de sauvegarde. Retrouvez plus d'informations à la section Création d'un fichier de sauvegarde à la page 262.

Les événements sont supprimés du journal des événements.

30.11 Création d'un fichier de sauvegarde

Lorsque vous supprimez des événements, vous pouvez créer un fichier de sauvegarde du rapport affiché dans la visionneuse des événements du SafeGuard Management Center.

1. Lors de la sélection de **Actions** > **Supprimer les événements** ou **Actions** > **Supprimer tous les événements**, la fenêtre **Sauvegarder les événements sous** permettant de créer un fichier de sauvegarde apparaît avant la suppression des événements.
2. Pour créer un fichier de sauvegarde .XML du journal des événements, entrez un nom et un emplacement de fichier, puis cliquez sur **OK**.

30.12 Ouverture d'un fichier de sauvegarde

1. Dans le SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Actions** > **Ouvrir le fichier de sauvegarde**.

   La fenêtre **Ouvrir une sauvegarde d'événement** apparaît.

3. Sélectionnez le fichier de sauvegarde à ouvrir et cliquez sur **Ouvrir**.

Le fichier de sauvegarde et les événements apparaissent dans la **Visionneuse des événements** du SafeGuard Management Center. Pour revenir à une vue standard de la **Visionneuse des événements**, cliquez de nouveau sur l'icône **Ouvrir le fichier de sauvegarde** dans la barre d'outils.

30.13 Nettoyage d'événement planifié par script

Remarque : le SafeGuard Management Center propose le **Planificateur de tâches** pour créer et planifier des tâches périodiques basées sur des scripts. Les tâches sont automatiquement exécutées par un service sur le serveur SafeGuard Enterprise pour exécuter les scripts spécifiées.

Quatre scripts SQL sont disponibles dans le répertoire \tools du produit SafeGuard Enterprise livré pour le nettoyage automatique et efficace du tableau EVENT :

- **`spShrinkEventTable_install.sql`**
- **`ScheduledShrinkEventTable_install.sql`**
- **`spShrinkEventTable_uninstall.sql`**
- **`ScheduledShrinkEventTable_uninstall.sql`**

Les deux scripts **`spShrinkEventTable_uninstall.sql`** et **`ScheduledShrinkEventTable_uninstall.sql`** permettent d'installer une procédure enregistrée ainsi qu'une tâche planifiée sur le serveur de la base de données. La tâche planifiée exécuté la procédure enregistrée à des intervalles réguliers définis. La procédure enregistrée déplace des événements du tableau EVENT dans le tableau de sauvegarde EVENT_BACKUP tout en conservant un nombre prédéfini d'événements récents dans le tableau EVENT.

Les deux scripts **`spShrinkEventTable_uninstall.sql`** et **`ScheduledShrinkEventTable_uninstall.sql`** permettent de désinstaller la procédure enregistrée ainsi que la tâche planifiée. Ces deux scripts suppriment également le tableau EVENT_BACKUP.

Remarque : si vous utilisez la procédure enregistrée pour déplacer des événements du tableau EVENT dans le tableau de sauvegarde, la connexion des événements ne s'applique plus. L'activation de la connexion tout en utilisant par ailleurs la procédure enregistrée pour le nettoyage des événements est inutile. Retrouvez plus d'informations à la section Connexion des événements journalisés à la page 261.

30.13.1 Création de la procédure enregistrée

Le script **`spShrinkEventTable_install.sql`** permet de créer une procédure enregistrée qui déplace des données du tableau EVENT dans un tableau de sauvegarde EVENT_BACKUP. Le tableau EVENT_BACKUP est créé automatiquement s'il n'existe pas.

La première ligne est "USE SafeGuard". Si vous avez donné un autre nom à votre base de données SafeGuard Enterprise, modifiez le nom en conséquence.

La procédure enregistrée conserve les **<n>** derniers événements dans le tableau EVENT et déplace les autres événements dans le tableau EVENT_BACKUP. Le nombre d'événements conservés dans le tableau EVENT est défini par un paramètre.

Pour exécuter la procédure stockée, lancez la commande suivante dans SQL Server Management Studio (Nouvelle requête) :

```
exec spShrinkEventTable 1000
```

Cet exemple de commande déplace tous les événements sauf les 1000 derniers.

30.13.2 Création d'une tâche planifiée d'exécution de la procédure enregistrée

Pour nettoyer automatiquement le tableau EVENT à intervalles réguliers, vous pouvez créer une tâche dans le serveur SQL. La tâche peut être créée avec le script **ScheduledShrinkEventTable_install.sql** ou à l'aide de SQL Enterprise Manager.

Remarque : la tâche planifiée ne s'applique pas aux bases de données SQL Express. L'agent SQL Server doit être en cours d'exécution pour que la tâche planifiée soit exécutée. SQL Server Express ne comportant aucun agent SQL Server, cette tâche ne s'applique pas à ces installations.

- Le script doit être exécuté dans msdb. Si vous avez donné un autre nom que SafeGuard à votre base de données SafeGuard Enterprise, modifiez le nom en conséquence.

  ```
  /* Default: Database name 'SafeGuard' change if required*/
  SELECT @SafeGuardDataBase='SafeGuard'
  ```

- Vous pouvez également préciser le nombre d'événements à conserver dans le tableau EVENT. Le nombre par défaut est 100 000.

  ```
  /* Default: keep the latest 100000 events, change if
  required*/
  SELECT @ShrinkCommand='exec spShrinkEventTable 100000'
  ```

- Vous pouvez spécifier si une exécution de tâche doit être journalisée dans le journal des événements NT.

  ```
  exec sp_add_job
  @job_name='AutoShrinkEventTable',
  @enabled=1,
  @notify_level_eventlog=3
  ```

  Les valeurs suivantes sont disponibles pour le paramètre **notify_level_eventlog** :

Valeur	Résultat
3	Journaliser à chaque exécution de la tâche.
2	Journaliser en cas d'échec de la tâche.
1	Journaliser, si la tâche a été exécutée avec succès.
0	Ne pas journaliser l'exécution de la tâche dans le journal des événements NT.

- Vous pouvez préciser la fréquence de répétition de la tâche en cas d'échec.

  ```
  exec sp_add_jobstep
  ```

  - **@retry_attempts=3**

    Cet exemple définit 3 tentatives d'exécution de la tâche en cas d'échec.

- **`@retry_interval=60`**

  Cet exemple définit un intervalle de 60 minutes.

- Vous pouvez spécifier l'heure d'exécution de la tâche.

  `exec sp_add_jobschedule`

  - **`@freq_type=4`**

    Cet exemple définit une exécution quotidienne de la tâche.

  - **`@freq_interval=1`**

    Cet exemple définit une exécution de la tâche une fois par jour.

  - **`@active_start_time=010000`**

    Cet exemple définit que la tâche est exécutée à 1 heure du matin.

Remarque : la syntaxe du paramètre **`@active_start_time`** indiquée ci-dessus fonctionne sous SQL Server 2005. La syntaxe correcte pour SQL Server 2000 est : **`@active_start_time='1:00:00'`**.

Remarque : outre les valeurs d'exemple indiquées ci-dessus, vous pouvez définir différentes options de planification avec **`sp_add-jobschedule`**. Par exemple, la tâche peut être exécutée toutes les deux minutes ou une fois par semaine seulement. Pour plus d'informations, consultez la documentation de Microsoft Transact SQL.

30.13.3 Nettoyage des procédures enregistrées, des tâches et des tableaux

Le script **`spShrinkEventTable_uninstall.sql`** permet de supprimer la procédure enregistrée et le tableau EVENT_BACKUP. Le script **`ScheduledShrinkEventTable_uninstall.sql`** permet d'annuler l'enregistrement de la tâche planifiée.

Remarque : lorsque vous exécutez **`spShrinkEventTable_uninstall.sql`**, le tableau EVENT_BACKUP est supprimé ainsi que toutes les données qu'il contient.

30.14 Modèles de messages de rapport

Les événements ne sont pas journalisés avec leurs textes d'événement complet dans la base de données SafeGuard Enterprise. Seuls l'identifiant et les valeurs de paramètre correspondantes sont inscrits dans le tableau de la base de données. Lors de la récupération des événements journalisés dans la **Visionneuse des événements** du SafeGuard Management Center, les valeurs de paramètre et les modèles de texte contenus dans le fichier .dll sont convertis en un texte d'événement complet dans la langue du système SafeGuard Management Center courant.

Les modèles utilisés pour les textes d'événement peuvent être modifiés et traités, à l'aide de requêtes SQL par exemple. Pour cela, vous pouvez générer une table contenant tous les modèles de texte des messages d'événement. Vous pouvez ensuite personnaliser les modèles en fonction de vos exigences particulières.

Pour créer une table contenant les modèles de texte des identifiants d'événement individuels :

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Options**.
2. Dans la fenêtre **Options**, accédez à l'onglet **Base de données**.
3. Dans la zone **Modèles de messages de rapport**, cliquez sur **Créer une table**.

La table contenant les modèles de l'identifiant d'événement est créée dans la langue système en cours et peut être personnalisée.

Remarque : la table doit être effacée avant la génération des modèles. Si les modèles ont été générés tel que décrit pour une langue spécifique et si un utilisateur génère les modèles d'une autre langue, les modèles de la première langue sont supprimés.

31 Planification des tâches

SafeGuard Management Center contient le **Planificateur de tâches** pour créer et planifier des tâches périodiques basées sur des scripts. Les tâches sont automatiquement exécutées par un service sur le serveur SafeGuard Enterprise pour exécuter les scripts spécifiées.

Les tâches périodiques sont, par exemple, utiles pour

- la synchronisation automatique entre Active Directory et SafeGuard Enterprise.
- la suppression automatique des journaux d'événements.

Pour ces deux procédures, des modèles de script prédéfinis sont disponibles avec SafeGuard Enterprise. Vous pouvez utiliser ces scripts tels quels ou les modifier en fonction de vos besoins. Retrouvez plus d'informations à la section Scripts prédéfinis pour les tâches quotidiennes à la page 273.

En tant que responsable de la sécurité avec les droits nécessaires, vous pouvez indiquer des scripts, des règles et des intervalles pour les tâches dans le **Planificateur des tâches**.

Remarque : assurez-vous que les autorisations SQL appropriées sont définies pour le compte qui sert à exécuter le **Planificateur de tâches** SafeGuard Enterprise. Retrouvez plus d'informations dans l'article de la base de connaissances suivant : http://www.sophos.com/fr-fr/support/knowledgebase/113582.aspx.

31.1 Création d'une nouvelle tâche

Pour créer des tâches dans le **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** s'affiche.

2. Cliquez sur **Créer...**.

   La boîte de dialogue **Nouvelle tâche** apparaît.

3. Dans le champ **Nom**, saisissez un nom de tâche unique.

   Si le nom de tâche n'est pas unique, un avertissement apparaît lorsque vous cliquez sur **OK** pour enregistrer la tâche.

4. Dans la liste déroulante du champ **Serveur SGN**, sélectionnez le serveur sur lequel la tâche doit fonctionner.

   La liste déroulante affiche seulement les serveurs pour lesquels la création de scripts est autorisée. Vous autorisez la création de scripts pour une serveur donné lorsque vous l'enregistrez dans l'**Outil de package de configuration** dans le SafeGuard Management Center. Retrouvez plus d'informations sur l'enregistrement des serveurs dans le *Guide d'installation de SafeGuard Enterprise*.

   Si vous sélectionnez **Aucune**, la tâche n'est pas exécutée.

5. Cliquez sur le bouton **Importer...** près du champ **Script**.

   La boîte de dialogue **Sélectionner le fichier script à importer** apparaît.

   Remarque : deux scripts prédéfinis sont disponibles dans le répertoire Script Templates de l'installation de votre SafeGuard Management Center. La boîte de dialogue **Sélectionner le fichier de script à importer** apparaît. Retrouvez plus d'informations à la section Scripts prédéfinis pour les tâches quotidiennes à la page 273.

   Dans le **Planificateur de tâches**, vous pouvez importer, exporter et modifier des scripts. Retrouvez plus d'informations à la section Utilisation de scripts dans le Planificateur de tâches à la page 272.

6. Sélectionnez le script que vous voulez exécuter avec la tâche et cliquez sur **OK**.

   Si le script sélectionné est vide, le bouton **OK** dans la boîte de dialogue reste désactivée et un avertissement apparaît.

7. Dans le champ **Heure de début**, spécifiez quand la tâche doit être exécutée sur le serveur sélectionnée.

   L'heure de début affichée est rendue à l'aide de l'heure locale de l'ordinateur sur lequel fonctionne le SafeGuard Management Center. En interne, l'heure de début est stockée en temps universel coordonné (UTC, Coordinated Universal Time). Ceci permet l'exécution de tâches au même moment, même si les serveurs sont dans différents fuseaux horaires. Tous les serveurs utilisent l'heure courante du serveur de base de données pour déterminer quand démarrer les tâches. Pour permettre une meilleure surveillance des tâches, l'heure de référence de la base de données apparaît dans la boîte de dialogue **Planificateur de tâches**.

8. Sous **Périodicité**, spécifiez à quelle fréquence la tâche doit être exécutée sur le serveur sélectionné.

   - Pour exécuter la tâche une fois, sélectionnez **Une seule fois** et spécifiez la **Date** requise.
   - Pour exécuter la tâche tous les jours, sélectionnez **Quotidien** suivi de **Chaque jour** (**y compris le samedi et le dimanche**) ou **Chaque jour de la semaine** (**du lundi au vendredi**).
   - Pour exécuter la tâche de façon hebdomadaire, sélectionnez **Hebdomadaire** et spécifiez le jour requis de la semaine.
   - Pour exécuter la tâche de façon mensuelle, sélectionnez **Mensuel** et spécifiez le jour requis du mois dans une plage de 1 à 31. Pour exécuter la tâche à la fin de chaque mois, sélectionnez **Dernier** dans la liste déroulante.

   Après avoir rempli tous les champs obligatoires, le bouton **OK** devient disponible.

9. Cliquez sur **OK**.

La tâche est enregistrée dans la base de données et apparaît dans l'aperçu du **Planificateur de tâches**. Elle est exécutée sur le serveur sélectionné en fonction de la planification spécifiée.

31.2 Affichage de l'aperçu du Planificateur de tâches

Après avoir créé des tâches à exécuter sur un serveur SafeGuard Enterprise, elles apparaissent dans la boîte de dialogue **Planificateur de tâches** que vous ouvrez en sélectionnant **Outils** > **Planificateur de tâches**.

Cette boîte de dialogue affiche pour chaque tâche les colonnes suivantes :

Colonne	Description
Nom de la tâche	Affiche le nom unique de la tâche.
Serveur SGN	Indique sur quel serveur la tâche est exécutée.
Planification	Afficher le programme spécifié pour la tâche avec la récurrence et l'heure.
Heure de la prochaine exécution	Affiche quand la prochaine exécution de la tâche aura lieu (date et heure). S'il n'existe plus d'heures d'exécution de cette tâche, cette colonne affiche **Aucune**.
Heure de la dernière exécution	Affiche quand la dernière exécution de la tâche aura lieu (date et heure). Si elle n'a pas encore été exécutée, cette colonne affiche **Aucune**.
Résultat de la dernière exécution	Affiche le résultat de la dernière tâche exécutée : ■ **Succès** Le script de la tâche a été exécuté avec succès. ■ **Échec** L'exécution de la tâche a échoué. Un numéro d'erreur apparaît, s'il est disponible. ■ **En cours d'exécution** Le script est en cours d'exécution. ■ **Droits insuffisants** La tâche a échoué à cause de droits insuffisants pour l'exécution de scripts. ■ **Interrompu** L'exécution de la tâche a été abandonnée car la durée d'exécution a dépassé 24 heures. ■ **Contrôle perdu** Le contrôle de l'exécution du script de la tâche a été perdu, par exemple parce que le service du planificateur SGN a été arrêté. ■ **Le script est corrompu**

Colonne	Description
	Le script à exécuter est corrompu. ■ **Le script a été supprimé entre-temps** Alors que la tâche était placée dans la file d'attente pour exécution, le script correspondant a été supprimé de la base de données SafeGuard Enterprise. ■ **Erreurs runtime** Une erreur runtime a été détectée lors du traitement du service du planificateur.

Sous les colonnes, les boutons suivants apparaissent :

Bouton	Description
Créer...	Cliquez sur ce bouton pour créer une nouvelle tâche.
Supprimer	Cliquez sur ce bouton pour supprimer une tâche sélectionnée.
Propriétés	Cliquez sur ce bouton pour afficher la boîte de dialogue **Propriétés de <nom de tâche>** d'une tâche sélectionnée. Dans cette boîte de dialogue, vous pouvez modifier la tâche ou importer, exporter et modifier des scripts.
Rafraîchir	Cliquez sur ce bouton pour rafraîchir la liste des tâches dans la boîte de dialogue **Planificateur de tâches**. Si un autre utilisateur a entre-temps ajouté ou supprimé des tâches, la liste est mise à jour.

Tous les serveurs utilisent l'heure courante du serveur de base de données pour déterminer quand démarrer les tâches. Ainsi, pour une meilleure surveillance des tâches, l'heure du serveur de base de données apparaît ici. Il apparaît avec l'heure locale de l'ordinateur sur lequel fonctionne le SafeGuard Management Center.

31.3 Modification de tâches

Pour modifier des tâches dans le **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

   La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Effectuez les changements requis.

   Remarque : ce nom de tâche doit être unique. Si vous changez le nom en un nom de tâche existant, un message d'erreur apparaît.

   Après avoir rempli tous les champs obligatoires, le bouton **OK** devient disponible.

4. Cliquez sur **OK**.

Les changements deviennent effectifs.

31.4 Suppression de tâches

Pour supprimer des tâches du **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise.

   Le bouton **Supprimer** devient disponible.

3. Cliquez sur le bouton **Supprimer** et confirmez que vous voulez supprimer la tâche.

La tâche est supprimée de la boîte de dialogue de l'aperçu du **Planificateur de tâches** et ne sera plus exécutée sur le serveur SafeGuard Enterprise.

Remarque : si la tâche a été démarrée entre-temps, elle est supprimée de la boîte de dialogue de l'aperçu du **Planificateur de tâches**, mais sera tout de même achevée.

31.5 Utilisation de scripts dans le Planificateur de tâches

Avec le **Planificateur de tâches**, vous pouvez importer, modifier et exporter des scripts. Pour utiliser les scripts dans le **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

31.5.1 Importation de scripts

Pour spécifier un script à exécuter par une tâche, le script doit être importé. Vous pouvez importer le script lorsque vous créez la tâche pour la première fois. Vous pouvez aussi importer des scripts pour les tâches existantes.

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

   La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Cliquez sur le bouton **Importer...** près du champ **Script**.

   La boîte de dialogue **Sélectionner le fichier script à importer** apparaît.

   Remarque : deux scripts prédéfinis sont disponibles dans le répertoire Script Templates de l'installation de votre SafeGuard Management Center. La boîte de dialogue **Sélectionner le fichier de script à importer** apparaît. Retrouvez plus d'informations à la section Scripts prédéfinis pour les tâches quotidiennes à la page 273.

4. Sélectionnez le script que vous voulez importer et cliquez sur **OK**.

   Le nom du script apparaît dans le champ **Script**.

5. Cliquez sur **OK**.

   Si le script a déjà été importé, vous êtes invité à confirmer que vous voulez remplacer l'ancien script.

   Si la taille du fichier à importer dépasse 10 Mo, un message d'erreur apparaît et le processus d'importation est rejeté.

Le script est enregistré dans la base de données.

31.5.2 Modification de scripts

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils** > **Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

   La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Cliquez sur le bouton déroulant **Modifier** près du champ **Script**.

   La liste déroulante montre tous les éditeurs disponibles pour la modification du script.

4. Sélectionnez l'éditeur que vous souhaitez utiliser.

   Le script s'ouvre dans l'éditeur sélectionné.

5. Effectuez vos changements et enregistrez-les.

   L'éditeur est fermé et la boîte de dialogue **Propriétés de <nom de tâche>** réapparaît.

6. Cliquez sur **OK**.

Le script changé est enregistré dans la base de données.

31.5.3 Exportation de scripts

1. Dans la barre de menus du SafeGuard Management Center, sélectionnez **Outils > Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

   La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Cliquez sur le bouton **Exporter...** près du champ **Script**.

   Une boîte de dialogue **Enregistrer sous** apparaît.

4. Sélectionnez l'emplacement du fichier pour l'enregistrement du script et cliquez sur **Enregistrer**.

   Le script est enregistré à l'emplacement de fichier spécifié.

31.5.4 Scripts prédéfinis pour les tâches périodiques

Les scripts prédéfinis suivants sont disponibles avec SafeGuard Enterprise :

- ActiveDirectorySynchronization.vbs

  Vous pouvez utiliser ce script pour la synchronisation automatique entre Active Directory et SafeGuard Enterprise.

- EventLogDeletion.vbs

  Vous pouvez utiliser ce script pour supprimer automatiquement les journaux d'événements.

Les scripts sont installés automatiquement dans le sous-dossier Script Templates de l'installation du SafeGuard Management Center.

Pour utiliser ces scripts lors de tâches quotidiennes, importez-les dans le **Planificateur de tâches** et apportez les changements de paramètres nécessaires avant de les utiliser.

31.5.4.1 Script prédéfini pour la synchronisation avec Active Directory

Vous pouvez importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise depuis un Active Directory. Retrouvez plus d'informations à la section Importation de la structure organisationnelle à la page 25.

Après avoir importé la structure du répertoire, vous pouvez planifier une tâche périodique de synchronisation automatique entre l'Active Directory et SafeGuard Enterprise. Pour cette tâche, vous pouvez utiliser le script prédéfini ActiveDirectorySynchronization.vbs.

Le script synchronise tous les conteneurs existants dans la base de données SafeGuard Enterprise avec un Active Directory.

Avant que nous n'utilisiez le script dans une tâche périodique, vous pouvez modifier les paramètres suivants :

Paramètre	Description
`logFileName`	Spécifiez un chemin pour le fichier journal du script. Ce paramètre est obligatoire. S'il est laissé vide ou incorrect, la synchronisation ne fonctionne pas et un message d'erreur apparaît. Par défaut, ce paramètre est vide. Si un fichier journal existe déjà, de nouveaux journaux sont ajoutés à la fin du fichier.
`synchronizeMembership`	Définissez ce paramètre sur 1 pour également synchroniser les appartenances. Si ce paramètre est défini sur 0, les appartenances ne sont pas synchronisées. Le paramètre par défaut est 1.
`synchronizeAccountState`	Définissez ce paramètre sur 1 pour également synchroniser l'état activé par l'utilisateur. Si ce paramètre est défini sur 0, l'état activé par l'utilisateur est seulement synchronisé à la première synchronisation. Le paramètre par défaut est 0.

Remarque : assurez-vous d'avoir les droits d'accès nécessaires pour la synchronisation Active Directory et que les autorisations SQL appropriées sont définies pour le compte utilisé pour exécuter le **Planificateur de tâches** SafeGuard Enterprise. Retrouvez plus d'informations à la section Droits d'accès du responsable de la sécurité et importation Active Directory à la page 27. Retrouvez plus d'informations sur la définition des droits d'accès Active Directory dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/107979.aspx. Retrouvez plus d'informations sur la définition des autorisations SQL dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/113582.aspx.

Une fois les droits définis correctement, appliquez les changements et redémarre le service : Passez sur le serveur hébergeant la page Web SafeGuard Enterprise. Ouvrez l'interface **Services** en cliquant sur **Démarrer** > **Exécuter** > **Services.msc**. Cliquez avec le bouton droit de la souris sur **Service du planificateur SafeGuard ®** et cliquez sur **Toutes les tâches**> **Redémarrer**.

Remarque : nous vous conseillons de synchroniser l'Active Directory à intervalles modérés, deux fois par jour maximum afin que les performances du serveur ne soient pas trop diminuées. Les nouveaux objets apparaîtront dans le SafeGuard Management Center sous .Autoregistered entre ces intervalles où ils peuvent être administrés normalement.

31.5.4.2 Script prédéfini pour la suppression automatique des journaux d'événements

Les événements journalisés dans la base de données SafeGuard Enterprise sont stockés dans le tableau EVENT. Retrouvez plus d'informations sur la journalisation à la section Rapports à la page 254.

Avec le **Planificateur de tâches**, vous pouvez créer une tâche périodique pour supprimer automatiquement les journaux d'événements. Pour cette tâche, vous pouvez utiliser le script prédéfini EventLogDeletion.vbs.

Le script supprime les événements du tableau EVENT. Si vous spécifiez le paramètre approprié, il déplace par ailleurs les événements dans le tableau de journalisation de sauvegarde EVENT_BACKUP en laissant un nombre prédéfini d'événements récents dans le tableau EVENT.

Avant que nous n'utilisiez le script dans une tâche périodique, vous pouvez modifier les paramètres suivants :

Paramètre	Description
maxDuration	Avec ce paramètre, spécifiez combien de temps (en jours) les événements doivent être conservés dans le tableau EVENT. Le nombre par défaut est 0. Si ce paramètre est défini sur 0, il n'y a pas de délai pour les événements conservés dans le tableau EVENT.
maxCount	Avec ce paramètre, spécifiez combien d'événements doivent rester dans le tableau EVENT. Le nombre par défaut est 5000. Si ce paramètre est défini sur 0, il n'y a pas de limite au nombre d'événements à conserver dans le tableau EVENT.
keepBackup	Avec ce paramètre, spécifiez si les événements supprimés doivent être sauvegardés dans le tableau EVENT. Le nombre par défaut est 0. Si ce paramètre est défini sur 0, les événements ne sont pas sauvegardés. Définissez ce paramètre sur 1 pour créer une sauvegarde des événements supprimés.

Remarque : si vous utilisez le script pour déplacer des événements du tableau EVENT dans le tableau de journalisation de sauvegarde, la connexion des événements ne s'applique plus. Pour activer la connexion aux événements tout en utilisant la procédure enregistrée pour le nettoyage des événements est inutile. Retrouvez plus d'informations à la section Connexion des événements journalisés à la page 261.

31.6 Restrictions concernant les serveurs enregistrés

Lorsque vous enregistrez des serveurs dans l'**Outil de package de configuration** du SafeGuard Management Center, vous pouvez enregistrer plus d'un modèle de serveur avec le même certificat de machine. Mais vous pouvez seulement installer un modèle à la fois sur la machine réelle.

Si la case à cocher **Scripts autorisés** est sélectionnée pour les deux serveurs, le **Planificateur de tâches** affiche les deux serveurs pour sélection dans la liste déroulante **Serveur SGN** des boîtes de dialogue **Nouvelle tâche** et **Propriétés de <nom de tâche>**. Le **Planificateur de tâches** ne peut pas déterminer lequel des deux modèles a été installé sur la machine.

Pour éviter cela, ne sélectionnez pas la case à cocher **Scripts autorisés** pour les modèles qui ne sont pas installés sur le serveur. Évitez aussi les modèles dupliqués avec le même certificat de machine.

Retrouvez plus d'informations sur l'enregistrement des serveurs dans le *Guide d'installation de SafeGuard Enterprise*.

31.7 Événements de journalisation du planificateur de tâches

Les événements concernant l'exécution des tâches peuvent être journalisés pour fournir des informations utiles, par exemple pour la résolution des problèmes. Vous pouvez définir les événements suivants à journaliser :

- La tâche du planificateur s'est exécutée avec succès
- La tâche du planificateur a échoué
- Le fil du service du planificateur s'est arrêté à cause d'une exception.

Les événements incluent les résultats de la console de scripts pour faciliter la résolution des problèmes.

Retrouvez plus d'informations sur la journalisation à la section Rapports à la page 254.

32 Gestion des ordinateurs d'extrémité Mac dans SafeGuard Management Center

Les Macs sur lesquels les produits Sophos suivants sont installés peuvent être gérés par SafeGuard Enterprise et/ou créer des rapports d'informations sur leur état. Les informations d'état apparaissent dans SafeGuard Management Center :

- Sophos SafeGuard File Encryption pour Mac 6.1
- Sophos SafeGuard Disk Encryption pour Mac 6.1
- Sophos SafeGuard Disk Encryption pour Mac 6 - rapport uniquement

Remarque :

Retrouvez plus de conseils et d'informations sur les spécificités et limites d'utilisation de SafeGuard File Encryption ou de SafeGuard Disk Encryption pour Mac dans le Manuel d'administration de Mac.

32.1 Données d'inventaire et d'état des Mac

Pour les Macs, l'**Inventaire** fournit les données suivantes sur chaque machine. Les données affichées peuvent varier selon le produit Sophos installé :

- Le nom du Mac
- Le système d'exploitation
- Le type de chiffrement
- L'état de l'authentification au démarrage
- Le nombre de lecteurs chiffrés
- Le nombre de lecteurs déchiffrés
- Le dernier contact du serveur
- La date de modification
- Si le certificat d'entreprise en cours est utilisé ou non

32.2 Création d'un package de configuration pour les Macs

Un package de configuration pour un Mac contient les informations sur le serveur et le certificat d'entreprise. Le Mac utilise ces informations pour signaler les informations d'état (authentification au démarrage SafeGuard active/inactive, état de chiffrement,...). Les informations d'état apparaissent dans SafeGuard Management Center.

1. Dans le menu **Outils** du SafeGuard Management Center, cliquez sur **Outil de package de configuration**.

2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Attribuez un serveur SafeGuard Enterprise principal (le serveur secondaire n'est pas nécessaire).
6. Sélectionnez **SSL** comme **Chiffrement du transport** pour la connexion entre l'ordinateur d'extrémité et le serveur SafeGuard Enterprise. **Sophos** en tant que **Chiffrement de transport** n'est pas pris en charge pour Mac.
7. Indiquez un chemin de sortie pour le package de configuration (ZIP).
8. Cliquez sur **Créer un package de configuration**.

   La connexion au serveur pour le mode **Chiffrement du transport** SSL est validé. En cas d'échec de la connexion, un message d'avertissement s'affiche.

Le package de configuration (ZIP) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer ce package sur vos Macs et le déployer sur ceux-ci.

33 SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique

Les disques durs à chiffrement automatique offrent un chiffrement de type matériel des données lorsqu'ils sont écrits sur le disque dur. Le Trusted Computing Group (TCG) a publié la norme Opal indépendante des fournisseurs pour les disques durs à chiffrement automatique. Différents fournisseurs de matériels proposent des disques durs compatibles Opal. SafeGuard Enterprise prend en charge la norme Opal et permet la gestion des ordinateurs d'extrémité avec disques durs compatibles Opal à chiffrement automatique. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/113366.aspx.

33.1 Comment SafeGuard Enterprise intègre-t-il les disques durs compatibles Opal ?

SafeGuard Enterprise permet aux ordinateurs d'extrémité de gérer les disques durs compatibles Opal à chiffrement automatique depuis SafeGuard Management Center, comme tout autre ordinateur d'extrémité protégé par SafeGuard Enterprise.

La gestion centralisée et pleinement transparente des disques durs compatibles Opal par SafeGuard Enterprise permet l'utilisation d'environnements informatiques hétérogènes. En prenant en charge la norme Opal, nous offrons la série complète des fonctions SafeGuard Enterprise aux utilisateurs professionnels des disques durs compatibles Opal à chiffrement automatique. Associé à SafeGuard Enterprise, les disques durs compatibles Opal offrent des fonctions de sécurité renforcées.

33.2 Amélioration des disques durs compatibles Opal avec SafeGuard Enterprise

En combinaison avec les disques durs compatibles Opal à chiffrement automatique, SafeGuard Enterprise offre les avantages suivants :

- Administration centralisée des ordinateurs d'extrémité
- Authentification au démarrage SafeGuard avec interface graphique utilisateur
- Prise en charge multi-utilisateurs
- Prise en charge de la connexion par token/carte à puce
- Prise en charge de la connexion par empreintes digitales
- Récupération (Local Self Help, Challenge/Réponse)
- Audit centralisé
- Chiffrement des supports amovibles (par exemple, les clés USB) avec SafeGuard Data Exchange

33.3 Administration avec SafeGuard Enterprise des ordinateurs d'extrémité équipés de disques durs compatibles Opal

Dans SafeGuard Management Center, vous pouvez administrer les ordinateurs d'extrémité équipés de disques durs compatibles Opal à chiffrement automatique comme tout autre poste protégé par SafeGuard Enterprise. En tant que responsable de la sécurité, vous pouvez définir des stratégies de sécurité, par exemple des stratégies d'authentification, et les déployer sur les ordinateurs d'extrémité.

Une fois qu'un ordinateur d'extrémité équipé d'un disque dur compatible Opal est enregistré dans SafeGuard Enterprise, des informations concernant l'utilisateur, l'ordinateur, le mode de connexion et le statut du chiffrement sont affichées. En outre, les événements sont consignés dans le journal.

Dans SafeGuard Enterprise, l'administration des ordinateurs d'extrémité équipés de disques durs compatibles Opal est transparente, ce qui signifie que les fonctions d'administration en général fonctionnent de la même façon que pour les autres ordinateurs d'extrémité protégés par SafeGuard Enterprise. Le type d'un ordinateur apparaît dans l'**Inventaire** d'un conteneur dans **Utilisateurs et ordinateurs**. La colonne **Type de chiffrement** vous indique si l'ordinateur correspondant est chiffré par SafeGuard Enterprise ou utilise un disque dur compatible Opal à chiffrement automatique.

33.4 Chiffrement de disques durs compatibles Opal

Les disques durs compatibles Opal sont à chiffrement automatique. Les données sont chiffrées automatiquement lorsqu'elles sont écrites sur le disque dur.

Les disques durs sont verrouillés par une clé AES 128/256 utilisée comme mot de passe Opal. Ce mot de passe est géré par SafeGuard Enterprise via une stratégie de chiffrement. Retrouvez plus d'informations à la section Verrouillage des disques durs compatibles Opal à la page 280.

33.5 Verrouillage des disques durs compatibles Opal

Pour verrouiller les disques durs compatibles Opal, la clé de la machine doit être définie pour au moins un volume sur le disque dur dans une stratégie de chiffrement. Au cas où la stratégie de chiffrement inclut un volume d'initialisation, la clé de la machine est définie automatiquement.

1. Dans le SafeGuard Management Center, créez une stratégie du type **Protection du périphérique**.
2. Dans le champ **Mode de chiffrement du support**, sélectionnez **Basé sur volume**.
3. Dans le champ **Clé à utiliser pour le chiffrement**, sélectionnez **Clé machine définie**.
4. Enregistrez vos changements dans la base de données.
5. Déployez la stratégie sur l'ordinateur d'extrémité correspondant.

Le disque dur compatible Opal est verrouillé et est seulement accessible en se connectant sur l'ordinateur à l'authentification au démarrage SafeGuard.

33.6 Autorisation de déverrouillage des disques durs compatibles Opal aux utilisateurs

En tant que responsable de la sécurité, vous pouvez permettre aux utilisateurs de déverrouiller les disques durs compatibles Opal sur les ordinateurs d'extrémité à l'aide de la commande **Déchiffrer** du menu contextuel Windows Explorer.

Condition préalable : dans la stratégie Protection des périphériques, ceci s'applique au disque dur Opal. L'option **L'utilisateur peut déchiffrer le volume** doit être définie sur **Oui**.

1. Dans SafeGuard Management Center, créez une stratégie du type **Protection des périphériques** et incluez tous les volumes présents sur le disque dur compatible Opal.
2. Dans le champ **Mode de chiffrement du support**, sélectionnez **Aucune chiffrement**.
3. Enregistrez vos changements dans la base de données.
4. Déployez la stratégie sur l'ordinateur d'extrémité correspondant.

L'utilisateur peut déverrouiller le disque dur compatible Opal sur l'ordinateur d'extrémité. Le disque dur demeure verrouillé.

33.7 Consignation dans le journal des événements pour les ordinateurs d'extrémité équipés de disques durs compatibles Opal

Les événements signalés par les ordinateurs d'extrémité équipés de disques durs compatibles Opal à chiffrement automatique sont consignés dans le journal, comme pour tout autre ordinateur d'extrémité protégé par SafeGuard Enterprise. Les événements ne mentionnent pas particulièrement le type d'ordinateur. Les événements signalés sont identiques à tout autre ordinateur d'extrémité protégé par SafeGuard Enterprise.

Retrouvez plus d'informations à la section Rapports à la page 254.

34 Événements disponibles pour les rapports

Le tableau suivant fournit un aperçu de tous les événements pouvant être sélectionnés pour la journalisation.

Catégorie	Identifiant d'événement	Description
Système	1005	Service démarré.
Système	1006	Échec du démarrage du service.
Système	1007	Arrêt du service.
Système	1016	Échec du test d'intégrité des fichiers de données.
Système	1017	Destination de journalisation non disponible.
Système	1018	Tentative non autorisée de désinstallation de SafeGuard Enterprise.
Authentification	2001	GINA externe identifié et intégré.
Authentification	2002	GINA externe identifié; échec de l'intégration.
Authentification	2003	Authentification au démarrage active.
Authentification	2004	Authentification au démarrage désactivée.
Authentification	2005	Éveil par appel réseau activé.
Authentification	2006	Éveil par appel réseau désactivé.
Authentification	2007	Challenge créé.
Authentification	2008	Réponse créée.
Authentification	2009	Connexion établie.
Authentification	2010	Échec de la connexion.
Authentification	2011	Utilisateur importé lors de la connexion et marqué comme propriétaire.
Authentification	2012	Utilisateur importé par un propriétaire et marqué comme non-propriétaire.
Authentification	2013	Utilisateur importé par un non-propriétaire et marqué comme non-propriétaire.
Authentification	2014	Utilisateur supprimé en tant que propriétaire.
Authentification	2015	Échec de l'importation de l'utilisateur lors de la connexion.
Authentification	2016	L'utilisateur s'est déconnecté.

Catégorie	Identifiant d'événement	Description
Authentification	2017	L'utilisateur a été contraint de se déconnecter.
Authentification	2018	Action effectuée sur le périphérique.
Authentification	2019	L'utilisateur a initié une modification de mot de passe/code PIN.
Authentification	2020	Modification mot de passe/code PIN de l'utilisateur après la connexion.
Authentification	2021	Qualité du mot de passe/code PIN.
Authentification	2022	La modification du mot de passe/code PIN n'a pas pu être effectuée.
Authentification	2023	LocalCache était corrompu et a été restauré.
Authentification	2024	Configuration non valide de la liste noire des mots de passe.
Authentification	2025	Le code de réponse permettant à l'utilisateur d'afficher le mot de passe a été reçu.
Authentification	2030	L'utilisateur connecté est un compte de service
Authentification	2035	Liste de comptes de service importée.
Authentification	2036	Liste de comptes de service supprimée.
Authentification	2056	Ajouter un utilisateur Windows de SGN
Authentification	2057	Supprimer des utilisateurs Windows de SGN d'une machine.
Authentification	2058	Suppression de l'utilisateur AUM
Authentification	2061	Code de renvoi de vérification Computrace.
Authentification	2062	Impossible d'exécuter la vérification Computrace.
Authentification	2071	L'initialisation du noyau a été menée à bien.
Authentification	2071	échec de l'initialisation du noyau.
Authentification	2073	Les clés machine ont été générées avec succès sur le client.
Authentification	2074	Les clés machine n'ont pas pu être générées avec succès sur le client. Code interne : 0x%1.
Authentification	2075	L'interrogation des propriétés du disque ou l'initialisation du disque Opal a échoué. Code interne : 0x%1.
Authentification	2079	L'importation de l'utilisateur dans le noyau a été menée à bien.
Authentification	2080	La suppression de l'utilisateur du noyau a été menée à bien.
Authentification	2081	Échec de l'importation de l'utilisateur dans le noyau.
Authentification	2082	Échec de la suppression de l'utilisateur du noyau.

Catégorie	Identifiant dévénement	Description
Authentification	2083	Réponse avec «afficher le mot de passe utilisateur» créée.
Authentification	2084	Réponse pour les clients virtuels créée.
Authentification	2085	Réponse pour les clients autonomes créée.
Authentification	2095	Impossible d'activer l'éveil par appel réseau.
Authentification		Un certificat a été attribué à l'utilisateur du client autonome.
Authentification	2096	Impossible de désactiver l'éveil par appel réseau.
Authentification	2097	L'utilisateur s'est connecté pour la première fois au client à l'aide du token de veille. Le token de veille a été défini comme clé standard.
Authentification	2098	L'activation du certificat de veille réussie a été signalée au serveur.
Authentification	2099	L'utilisateur s'est connecté pour la première fois au client à l'aide du token de veille. Le certificat de veille n'a pas pu être activé à cause d'une erreur.
Authentification	2100	L'activation du certificat de veille a échoué sur le serveur.
Administration	2500	Lancement de SafeGuard Enterprise Administration.
Administration	2501	Échec de la connexion à SafeGuard Enterprise Administration.
Administration	2502	Autorisation pour SafeGuard Enterprise Administration refusée.
Administration	2504	Autorisation supplémentaire accordée pour l'action.
Administration	2505	Autorisation supplémentaire refusée.
Administration	2506	Importation de données depuis le répertoire menée à bien.
Administration	2507	Importation de données depuis le répertoire annulée.
Administration	2508	Impossible d'importer des données depuis le répertoire.
Administration	2511	Utilisateur créé.
Administration	2513	Utilisateur modifié.
Administration	2515	Utilisateur supprimé.
Administration	2518	Échec de l'application de l'utilisateur.
Administration	2522	Impossible de supprimer l'utilisateur.
Administration	2525	Machine appliquée.
Administration	2529	Machine supprimée.
Administration	2532	Échec de l'application de la machine.
Administration	2536	Impossible de supprimer la machine.

Catégorie	Identifiant d'événement	Description
Administration	2539	OU appliqué.
Administration	2543	OU supprimé.
Administration	2546	Échec de l'application de l'OU.
Administration	2547	Échec de l'importation de l'OU.
Administration	2550	Échec de suppression de l'OU.
Administration	2553	Groupe appliqué.
Administration	2555	Groupe modifié.
Administration	2556	Groupe renommé.
Administration	2557	Groupe supprimé.
Administration	2560	Échec de l'application du groupe.
Administration	2562	Impossible de modifier le groupe.
Administration	2563	Impossible de renommer le groupe.
Administration	2564	Impossible de supprimer le groupe.
Administration	2573	Membres ajoutés au groupe.
Administration	2575	Membres supprimés du groupe.
Administration	2576	Impossible d'ajouter les membres au groupe.
Administration	2578	Impossible de supprimer les membres du groupe.
Administration	2580	Groupe déplacé d'une OU vers un autre.
Administration	2583	Impossible de passer le groupe d'une OU vers un autre.
Administration	2591	Objets ajoutés au groupe.
Administration	2593	Objets supprimés du groupe.
Administration	2594	Impossible d'ajouter les objets au groupe.
Administration	2596	Impossible de supprimer les objets du groupe.
Administration	2603	Clé générée. Algorithme.
Administration	2607	Clé attribuée.
Administration	2608	Attribution de clé annulée.
Administration	2609	Impossible de générer la clé.
Administration	2613	Impossible d'attribuer la clé.
Administration	2614	Impossible de supprimer l'attribution de la clé.

Catégorie	Identifiant d'événement	Description
Administration	2615	Certificat généré.
Administration	2616	Certificat importé.
Administration	2619	Certificat supprimé.
Administration	2621	Certificat attribué à l'utilisateur.
Administration	2622	Annulation de l'attribution de certificat à l'utilisateur.
Administration	2623	Impossible de créer le certificat.
Administration	2624	Impossible d'importer le certificat.
Administration	2627	Impossible de supprimer le certificat.
Administration	2628	Échec de l'extension du certificat.
Administration	2629	Impossible d'attribuer le certificat à l'utilisateur.
Administration	2630	Impossible de supprimer l'attribution du certificat à l'utilisateur.
Administration	2631	token connecté.
Administration	2632	token supprimé.
Administration	2633	token généré pour l'utilisateur.
Administration	2634	Changer le code PIN utilisateur sur le token.
Administration	2635	Changer le code PIN SO sur le token.
Administration	2636	token verrouillé.
Administration	2637	token déverrouillé.
Administration	2638	token supprimé.
Administration	2639	Attribution de token supprimée pour l'utilisateur.
Administration	2640	Impossible de générer un token pour l'utilisateur.
Administration	2641	Impossible de modifier le code PIN utilisateur sur le token.
Administration	2642	Impossible de modifier le code PIN SO sur le token.
Administration	2643	Impossible de verrouiller le token.
Administration	2644	Impossible de déverrouiller le token.
Administration	2645	Impossible de supprimer le token.
Administration	2647	Stratégie créée.
Administration	2648	Stratégie modifiée.
Administration	2650	Stratégie supprimée.

Catégorie	Identifiant d'événement	Description
Administration	2651	Stratégie attribuée et activée sur l'OU.
Administration	2652	Stratégie attribuée supprimée de l'OU.
Administration	2653	Impossible de créer la stratégie.
Administration	2654	Impossible de modifier la stratégie.
Administration	2657	Échec d'attribution et d'activation d'une stratégie dans l'OU.
Administration	2658	Échec de la suppression de la stratégie attribuée de l'OU.
Administration	2659	Groupe de stratégies créé.
Administration	2660	Groupe de stratégies modifié.
Administration	2661	Groupe de stratégies supprimé.
Administration	2662	Impossible de créer le groupe de stratégies.
Administration	2663	Impossible de modifier le groupe de stratégies.
Administration	2665	La stratégie suivante a été ajoutée au groupe de stratégies.
Administration	2667	La stratégie suivante a été supprimée du groupe de stratégies.
Administration	2668	Impossible d'ajouter la stratégie au groupe de stratégies.
Administration	2670	Impossible de supprimer la stratégie du groupe de stratégies.
Administration	2678	Événement enregistré exporté.
Administration	2679	Échec d'exportation des événements enregistrés.
Administration	2680	Événements enregistrés supprimés.
Administration	2681	Impossible de supprimer les événements enregistrés.
Administration	2684	Le responsable de la sécurité autorise le renouvellement du certificat.
Administration	2685	Le responsable de la sécurité refuse le renouvellement du certificat.
Administration	2686	Impossible de modifier les paramètres de renouvellement du certificat.
Administration	2687	Modification du certificat du responsable.
Administration	2688	Impossible de modifier le certificat du responsable.
Administration	2692	Création de groupes de travail.
Administration	2693	Création de groupes de travail impossible.
Administration	2694	Suppression de groupes de travail.
Administration	2695	Suppression de groupes de travail impossible.

Catégorie	Identifiant dévénement	Description
Administration	2696	Création d'utilisateurs.
Administration	2697	Création d'utilisateurs impossible.
Administration	2698	Création de machines.
Administration	2699	Création de machines impossible.
Administration	2700	Violation de la licence.
Administration	2701	Création du fichier de clé.
Administration	2702	Suppression de la clé du fichier de clé.
Administration	2703	Le responsable de la sécurité a désactivé l'authentification au démarrage dans la stratégie.
Administration	2704	Sujet de la question LSH créé.
Administration	2705	Sujet de la question LSH modifié.
Administration	2706	Sujet de la question LSH supprimé.
Administration	2707	Question modifiée.
Administration	2753	Accès en lecture seule au conteneur '%1' accordé pour le responsable de la sécurité '%2'.
Administration	2755	Accès complet au conteneur '%1' accordé pour le responsable de la sécurité '%2'.
Administration	2757	Accès complet au conteneur '%1' révoqué pour le responsable de la sécurité '%2'.
Administration	2766	Accès au conteneur '%1' explicitement refusé pour le responsable de la sécurité '%2'.
Administration	2767	Accès explicitement refusé au conteneur '%1' révoqué pour le responsable de la sécurité '%2'.
Administration	2768	Accès en lecture seule au conteneur '%1' révoqué pour le responsable de la sécurité '%2'.
Administration	2810	Utilisateur POA "%1" créé.
Administration	2811	Utilisateur POA "%1" modifié.
Administration	2812	Utilisateur POA "%1" supprimé.
Administration	2815	Échec de la création de l'utilisateur POA "%1".
Administration	2816	Échec de la modification de l'utilisateur POA "%1".
Administration	2817	Échec de la suppression de l'utilisateur POA "%1".
Administration	2820	Groupe POA "%1" créé.

Catégorie	Identifiant dévénement	Description
Administration	2821	Groupe POA "%1" modifié.
Administration	2822	Groupe POA "%1" supprimé.
Administration	2825	Échec de la création du groupe POA "%1".
Administration	2826	Échec de la modification du groupe POA "%1".
Administration	2827	Échec de la suppression du groupe POA "%1".
Administration	2850	Le service du planificateur s'est arrêté à cause d'une exception.
Administration	2851	La tâche du planificateur s'est exécutée avec succès.
Administration	2852	Échec de la tâche du planificateur.
Administration	2853	Tâche du planificateur créée ou modifiée.
Administration	2854	Tâche du planificateur supprimée.
Client	3003	Sauvegarde du noyau réussie.
Client	3005	Première tentative de restauration du noyau réussie.
Client	3006	Deuxième tentative de restauration du noyau réussie.
Client	3007	Échec de la sauvegarde du noyau.
Client	3008	Échec de la restauration du noyau.
Client	3030	L'utilisateur a modifié ses secrets LSH après la connexion.
Client	3035	Activation de LSH.
Client	3040	Désactivation de LSH.
Client	3045	LSH est disponible : client Enterprise
Client	3046	LSH est disponible : client autonome
Client	3050	Désactivation de LSH : client Enterprise
Client	3051	LSH n'est pas disponible : client autonome
Client	3055	La liste QST (questions LSH) a été modifiée.
Client	3405	La désinstallation du client de protection de configuration a échoué.
Client	3070	La sauvegarde de clé a été enregistrée dans le partage réseau spécifié.
Client	3071	La sauvegarde de clé n'a pas pu être enregistrée dans le partage réseau spécifié.
Client	3110	Utilisateur POA "%1" importé dans la POA.
Client	3111	Utilisateur POA "%1" supprimé de la POA.

Catégorie	Identifiant d'événement	Description
Client	3115	Utilisateur POA "%1" a changé le mot de passe via la touche F8.
Client	3116	Échec de l'importation de l'utilisateur POA "%1" dans la POA.
Client	3117	Échec de la suppression de l'utilisateur POA "%1" de la POA.
Client	3118	Utilisateur POA "%1" : échec de la modification du mot de passe via la touche F8.
Client	3406	Une erreur s'est produite au niveau du client de protection de configuration.
Client	3407	Le client de protection de configuration a détecté une possible falsification.
Client	3408	Le client de protection de configuration a détecté une possible falsification des fichiers journaux.
Chiffrement	3501	Accès refusé au support sur le lecteur.
Chiffrement	3502	Accès refusé au fichier de données.
Chiffrement	3503	Démarrage du chiffrement initial basé sur secteur du lecteur
Chiffrement	3504	Démarrage du chiffrement initial basé sur secteur du lecteur (mode rapide).
Chiffrement	3505	Fin du chiffrement initial basé sur secteur du lecteur réussie.
Chiffrement	3506	Échec et clôture du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3507	Annulation du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3508	Échec du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3509	Démarrage du déchiffrement basé sur secteur du lecteur.
Chiffrement	3510	Clôture du déchiffrement basé sur secteur du lecteur réussie.
Chiffrement	3511	Échec et clôture du déchiffrement basé sur secteur du lecteur.
Chiffrement	3512	Annulation du déchiffrement basé sur secteur du lecteur.
Chiffrement	3513	Échec du déchiffrement basé sur secteur du lecteur.
Chiffrement	3514	Démarrage du chiffrement initial F&F sur le lecteur.
Chiffrement	3515	Fin du chiffrement initial F&F sur le lecteur réussie.
Chiffrement	3516	Échec et clôture du chiffrement initial F&F sur le lecteur.
Chiffrement	3517	Annulation du déchiffrement F&F sur le lecteur.
Chiffrement	3519	Démarrage du chiffrement F&F.
Chiffrement	3520	Clôture du chiffrement F&F réussie.

Catégorie	Identifiant d'événement	Description
Chiffrement	3521	Échec et clôture du déchiffrement F&F.
Chiffrement	3522	Annulation du déchiffrement F&F sur le lecteur.
Chiffrement	3524	Démarrage du chiffrement F&F.
Chiffrement	3525	Fin du chiffrement F&F réussie.
Chiffrement	3526	Échec du chiffrement F&F.
Chiffrement	3540	Démarrage du déchiffrement F&F.
Chiffrement	3541	Fin du déchiffrement F&F réussie.
Chiffrement	3542	Échec du déchiffrement F&F.
Chiffrement	3543	Sauvegarde de la clé d'initialisation réussie.
Chiffrement	3544	Nombre maximum d'algorithmes d'initialisation dépassé.
Chiffrement	3545	Erreurs de lecture sur la KSA.
Chiffrement	3546	Désactivation des volumes en fonction des stratégies définies.
Chiffrement	3547	Avertissement ! La sauvegarde du secteur de démarrage NTFS manque sur le volume %1.
Chiffrement	3560	Contrôle d'accès
Chiffrement	3600	Erreur générale de chiffrement
Chiffrement	3601	Erreur de chiffrement - moteur: volume manquant.
Chiffrement	3602	Erreur de chiffrement - moteur: volume hors ligne.
Chiffrement	3603	Erreur de chiffrement - moteur: volume supprimé.
Chiffrement	3604	Erreur de chiffrement - moteur: volume incorrect.
Chiffrement	3607	Erreur de chiffrement - clé de chiffrement manquante.
Chiffrement	3610	Erreur de chiffrement - zone de stockage des clés d'origine endommagée
Chiffrement	3611	Erreur de chiffrement - zone de stockage des clés de sauvegarde endommagée sur le volume
Chiffrement	3612	Erreur de chiffrement - zone ESA d'origine endommagée sur le volume
Contrôle d'accès	4400	Le port a été approuvé.
Contrôle d'accès	4401	Le périphérique a été approuvé.
Contrôle d'accès	4402	Le périphérique de stockage a été approuvé.
Contrôle d'accès	4403	Le réseau local sans fil a été approuvé.

Catégorie	Identifiant d'événement	Description
Contrôle d'accès	4404	Le port a été retiré avec succès.
Contrôle d'accès	4405	Le périphérique a été retiré avec succès.
Contrôle d'accès	4406	Le périphérique de stockage a été retiré avec succès.
Contrôle d'accès	4407	Le réseau local sans fil a été déconnecté avec succès.
Contrôle d'accès	4408	Port restreint
Contrôle d'accès	4409	Périphérique restreint
Contrôle d'accès	4410	Périphérique de stockage restreint
Contrôle d'accès	4411	Réseau local sans fil restreint
Contrôle d'accès	4412	Port bloqué
Contrôle d'accès	4413	Périphérique bloqué
Contrôle d'accès	4414	Périphérique de stockage bloqué
Contrôle d'accès	4415	Réseau local sans fil bloqué

35 Codes d'erreur

35.1 Codes SGMERR du journal des événements de Windows

Le message suivant s'affichera dans le journal des événements de Windows :

"Autorisation pour l'administration de SafeGuard Enterprise refusée pour l'utilisateur... Raison : SGMERR[536870951]».

Consultez le tableau ci-dessous pour connaître la définition du numéro "536870951". Le numéro "536870951" signifie par exemple "Saisie incorrecte du code PIN. Authentification impossible de l'utilisateur."

Identifiant de l'erreur	Affichage
0	OK
21	Erreur interne détectée
22	Module non initialisé
23	Erreur d'E/S de fichier détectée
24	Le cache ne peut pas être attribué
25	Erreur de lecture d'E/S de fichier
26	Erreur d'écriture d'E/S de fichier
50	Aucune opération n'a été effectuée
101	Erreur générale
102	Accès refusé
103	Le fichier existe déjà
1201	Impossible d'ouvrir l'entrée du registre.
1202	Impossible de lire l'entrée du registre.
1203	Impossible d'écrire l'entrée du registre.
1204	Impossible de supprimer l'entrée du registre.
1205	Impossible de créer l'entrée du registre.
1206	Accès impossible à un pilote ou un service système.
1207	Impossible d'ajouter un pilote ou un service système dans le registre.
1208	Impossible de supprimer un pilote ou un service système du registre.
1209	Une entrée est déjà présente dans le registre pour un pilote ou un service système.

Identifiant de l'erreur	Affichage
1210	Aucun accès au Service Control Manager.
1211	Impossible de trouver une entrée dans le registre pour une session.
1212	Une entrée du registre est non valide ou erronée.
1301	Échec de l'accès à un lecteur.
1302	Aucune information n'est disponible sur un volume.
1303	Échec de l'accès à un volume.
1304	Option non valide définie.
1305	Type de système de fichiers non valide.
1306	Le système de fichiers existant sur un volume et le système de fichiers défini diffèrent.
1307	La taille du cluster existant utilisée par un système de fichiers et la taille du cluster définie diffèrent.
1308	Taille de secteur non valide utilisée par un système de fichiers défini.
1309	Secteur de départ non valide défini.
1310	Type de partition non valide défini.
1311	Impossible de trouver une zone non utilisée et défragmentée de la taille requise sur un volume.
1312	Impossible de marquer le cluster du système de fichiers comme étant utilisé.
1313	Impossible de marquer le cluster du système de fichiers comme étant utilisé.
1314	Impossible de marquer le cluster du système de fichiers comme étant CORRECT.
1315	Impossible de marquer le cluster du système de fichiers comme étant INCORRECT.
1316	Aucune information disponible sur les clusters d'un système de fichiers.
1317	Impossible de trouver une zone marquée comme MAUVAISE sur un volume.
1318	Taille non valide d'une zone sur un volume défini.
1319	Le secteur MBR d'un disque dur n'a pas pu être remplacé.
1330	Une commande erronée a été définie pour une allocation ou une désallocation.
1351	Algorithme non valide défini.
1352	Échec de l'accès au noyau système.
1353	Aucun noyau système n'est installé.
1354	Une erreur s'est produite lors de l'accès au noyau système.

Identifiant de l'erreur	Affichage
1355	Modification non valide des paramètres système.
1401	Échec de l'écriture de données sur un lecteur.
1402	Échec de la lecture de données d'un lecteur.
1403	Échec de l'accès à un lecteur.
1404	Lecteur non valide défini.
1405	Échec du changement de position sur un lecteur.
1406	Le lecteur n'est pas prêt.
1407	Échec du démontage d'un lecteur.
1451	Impossible d'ouvrir le fichier.
1452	Le fichier est introuvable.
1453	Le chemin d'accès défini pour le fichier est non valide.
1454	Impossible de créer le fichier.
1455	Impossible de copier le fichier.
1456	Aucune information n'est disponible sur un volume.
1457	Impossible de modifier la position dans un fichier.
1458	Échec de la lecture de données d'un fichier.
1459	Échec de l'écriture de données dans un fichier.
1460	Impossible de supprimer un fichier.
1461	Système de fichiers non valide.
1462	Impossible de fermer le fichier.
1463	L'accès à un fichier a été refusé.
1501	Mémoire disponible insuffisante.
1502	Paramètre non valide ou erroné défini.
1503	Dépassement de la taille de la mémoire tampon de données.
1504	Un module DLL n'a pas pu être chargé.
1505	Une fonction ou un processus a été annulé.
1506	Aucun accès autorisé.
1510	Aucun noyau système n'est installé.
1511	Impossible de lancer un programme.

Identifiant de l'erreur	Affichage
1512	Une fonction, un objet ou une donnée est indisponible.
1513	Entrée non valide détectée.
1514	Un objet existe déjà.
1515	Appel de fonction non valide.
1516	Une erreur interne s'est produite.
1517	Une violation d'accès s'est produite.
1518	La fonction ou le mode n'est pas pris en charge.
1519	Échec de la désinstallation.
1520	Une erreur d'exception s'est produite.
1550	Le secteur MBR du disque dur n'a pas pu être remplacé.
2850	Le service du planificateur s'est arrêté à cause d'une exception.
2851	La tâche du planificateur s'est exécutée avec succès.
2852	Échec de la tâche du planificateur.
2853	Tâche du planificateur créée ou modifiée.
2854	Tâche du planificateur supprimée.
20001	Inconnu
20002	Processus terminé
20003	Fichier non vérifié
20004	Stratégie non valide
30050	Impossible d'ouvrir la commande
30051	Mémoire insuffisante
30052	Échec général de la communication de traitement
30053	Une ressource est temporairement indisponible. Cet état est temporaire. Des tentatives d'accès ultérieures peuvent fonctionner normalement.
30054	Échec général de communication
30055	Valeur renvoyée inattendue
30056	Aucun lecteur de carte n'est connecté.
30057	Dépassement de mémoire tampon
30058	La carte n'est pas alimentée
30059	Un dépassement de délai s'est produit

Identifiant de l'erreur	Affichage
30060	Type de carte incorrect
30061	La fonctionnalité demandée n'est pas prise en charge à l'heure actuelle / par ce SE / dans cette situation, etc.
30062	Pilote non valide
30063	Ce logiciel ne peut pas utiliser le microprogramme du matériel connecté
30064	Impossible d'ouvrir le fichier
30065	Fichier introuvable
30066	La carte n'est pas insérée
30067	Argument non valide
30068	Le sémaphore est en cours d'utilisation
30069	Le sémaphore est temporairement en cours d'utilisation
30070	Échec général
30071	Actuellement, vous ne disposez pas des droits permettant d'effectuer l'opération demandée. Généralement, un mot de passe doit être fourni au préalable.
30072	Actuellement, le service n'est pas disponible
30073	Un élément (par exemple, une clé portant un nom spécifique) est introuvable
30074	Le mot de passe fourni est incorrect.
30075	Le mot de passe fourni plusieurs fois est incorrect, l'accès est par conséquent verrouillé. Il est généralement possible d'utiliser un outil d'administration approprié pour le déverrouiller.
30076	L'identité ne correspond pas à une identité définie ayant fait l'objet d'un contrôle croisé
30077	Plusieurs erreurs se sont produites. Utilisez ce code d'erreur si c'est le seul moyen d'obtenir un code d'erreur lorsque des erreurs différentes se sont produites.
30078	Il reste des éléments, par conséquent la structure du répertoire ne peut par exemple pas être supprimée.
30079	Erreur lors du contrôle de cohérence
30080	L'identifiant se trouve sur une liste noire, par conséquent, l'opération demandée n'est pas autorisée.
30081	Identificateur non valide
30082	Fichier de configuration non valide
30083	Secteur introuvable.
30084	Entrée introuvable.

Identifiant de l'erreur	Affichage
30085	Plus de sections
30086	Fin du fichier atteinte.
30087	L'élément spécifié existe déjà
30088	Le mot de passe fourni est trop court.
30089	Le mot de passe fourni est trop long.
30090	Un élément (par exemple, un certificat) a expiré.
30091	Le mot de passe n'est pas verrouillé.
30092	Chemin introuvable.
30093	Le répertoire n'est pas vide.
30094	Aucune donnée supplémentaire
30095	Le disque est plein.
30096	Une opération a été annulée.
30097	Données en lecture seule ; une opération d'écriture a échoué
12451840	La clé n'est pas disponible.
12451842	La clé n'est pas définie.
12451842	Accès refusé au support non chiffré.
12451843	Accès refusé au support non chiffré sauf s'il est vide.
352321637	Le fichier n'est pas chiffré.
352321638	La clé n'est pas disponible.
352321639	La clé correcte n'est pas disponible.
352321640	Erreur de la somme de contrôle dans l'en-tête du fichier.
352321641	Erreur de la fonction CBI.
352321642	Nom de fichier non valide.
352321643	Erreur de lecture/écriture du fichier temporaire.
352321644	L'accès aux données non chiffrées n'est pas autorisé.
352321645	Zone de stockage des clés (KSA) saturée.
352321646	Le fichier est déjà chiffré avec un autre algorithme.
352321647	Le fichier est compressé avec NTFS et ne peut pas être chiffré.
352321648	Le fichier est chiffré avec EFS.

Identifiant de l'erreur	Affichage
352321649	Propriétaire du fichier non valide
352321650	Mode de chiffrement du fichier non valide
352321651	Erreur d'opération CBC.
385875969	Intégrité rompue.
402653185	Le token ne contient pas de codes d'accès.
402653186	Impossible d'écrire les codes d'accès sur le token.
402653187	Impossible de créer la balise TDF.
402653188	La balise TDF ne contient pas les données requises.
402653189	L'objet existe déjà sur le token.
402653190	Aucun connecteur valide trouvé
402653191	Lecture impossible du numéro de série
402653192	Le chiffrement du token a échoué.
402653193	Le déchiffrement du token a échoué.
536870913	Le fichier de clé ne contient pas de données valides.
536870914	Des parties de la paire de clés RSA sont incorrectes
536870915	Impossible d'importer la paire de clés.
536870916	Le format du fichier de clé n'est pas valide.
536870917	Aucune donnée disponible
536870918	Échec de l'importation du certificat.
536870919	Le module a déjà été initialisé
536870920	Le module n'a pas encore été initialisé
536870921	Le chiffrement ASN.1 est corrompu.
536870922	Longueur des données incorrecte
536870923	Signature incorrecte.
536870924	Mécanisme de chiffrement appliqué incorrect.
536870925	Cette version n'est pas prise en charge.
536870926	Erreur de remplissage.
536870927	Indicateurs non valides.
536870928	Le certificat a expiré et n'est plus valide

Identifiant de l'erreur	Affichage
536870929	Heure saisie incorrecte. Le certificat n'est pas encore valide.
536870930	Le certificat a été retiré.
536870931	La chaîne de certificat est non valide.
536870932	Impossible de créer la chaîne de certificat.
536870933	Impossible de contacter CDP.
536870934	Un certificat pouvant être utilisé uniquement comme unité de donnée finale a été utilisé comme CA ou réciproquement.
536870935	Problèmes de validité de la longueur du certificat dans la chaîne.
536870936	Erreur d'ouverture d'un fichier.
536870937	Erreur de lecture d'un fichier.
536870938	Un ou plusieurs paramètres attribués à la fonction sont incorrects.
536870939	Le résultat de la fonction dépasse la taille du cache.
536870940	Problème de token et/ou de connecteur rompu.
536870941	Le token n'a pas suffisamment de mémoire pour effectuer la fonction demandée.
536870942	Le token a été retiré du connecteur alors que la fonction était en cours.
536870943	La fonction demandée n'a pas pu être réalisée, mais aucune information concernant la cause de cette erreur n'est disponible.
536870945	L'ordinateur sur lequel la compilation CBI s'effectue n'a pas suffisamment de mémoire pour effectuer la fonction demandée. Il se peut que cette fonction ne soit que partiellement exécutée.
536870946	Une opération demandée n'est pas prise en charge par la compilation CBI.
536870947	Tentative de définition d'une valeur pour un objet qui ne peut pas être paramétré ou modifié.
536870948	Valeur non valide pour l'objet.
536870949	Échec d'obtention de la valeur d'un objet car celui-ci est sensible ou inaccessible.
536870950	Le code PIN saisi a expiré. (Le fait que le code PIN d'un utilisateur classique fonctionne ou non sur un token générée dépend de cette dernière).
536870951	Le code PIN fourni est incorrect. Authentification impossible de l'utilisateur.
536870952	Le code PIN saisi contient des caractères non valides. Ce code de réponse ne s'applique qu'aux opérations qui tentent de définir un code PIN.
536870953	Le code PIN saisi est trop long ou trop court. Ce code de réponse ne s'applique qu'aux opérations qui tentent de définir un code PIN.

Identifiant de l'erreur	Affichage
536870954	Le code PIN sélectionné est bloqué et ne peut pas être utilisé. Ceci se produit lorsqu'un certain nombre de tentatives ont été faites pour authentifier un utilisateur et lorsque le token refuse toute tentative supplémentaire.
536870955	Identifiant de connecteur non valide.
536870956	Le token n'était pas dans le connecteur lors de la requête.
536870957	L'archive CBI et/ou le connecteur n'ont pas reconnu le token qui s'y trouve.
536870958	L'opération demandée n'a pas pu être effectuée car le token est protégé en écriture.
536870959	L'utilisateur saisi ne peut pas être connecté car il a déjà ouvert une session.
536870960	L'utilisateur saisi ne peut pas se connecter car un autre utilisateur est déjà connecté à cette session.
536870961	L'opération demandée n'a pas pu être effectuée car aucun utilisateur correspondant n'est connecté. Par exemple, il n'est pas possible de quitter une session lorsqu'un utilisateur est encore connecté.
536870962	Le code PIN de l'utilisateur normal n'a pas été initialisé avec CBIInitPin
536870963	Une tentative de connexion effectuée par plusieurs utilisateurs simultanément sur le même token a été autorisée.
536870964	Une valeur incorrecte a été spécifiée en tant que CBIUser. Les types valides sont définis dans les types d'utilisateurs.
536870965	Un objet ayant l'identifiant spécifié est introuvable sur le token.
536870966	Dépassement de délai de l’opération.
536870967	Cette version d'IE n'est pas prise en charge
536870968	Échec d'authentification
536870969	Le certificat de base n'est pas sécurisé.
536870970	Aucune CRL trouvée
536870971	Aucune connexion Internet active.
536870972	Erreur de valeur de temps du certificat.
536870973	Impossible de vérifier le certificat sélectionné.
536870974	Le statut d'expiration du certificat est inconnu.
536870975	Le module s'est fermé. Aucune autre demande.
536870976	Une erreur s'est produite pendant la requête d'une fonction réseau.
536870977	Une requête de fonction non valide a été reçue.
536870978	Impossible de trouver un objet.

Identifiant de l'erreur	Affichage
536870979	Une session terminal server a été interrompue.
536870980	Opération non valide.
536870981	L'objet est en cours d'utilisation
536870982	Le générateur de nombres aléatoire n'a pas été initialisé. (CBIRNDInit ( ) non requis.)
536870983	Commande inconnue (voir CBIControl ( ))
536870984	UNICODE n'est pas pris en charge
536870985	Davantage de valeurs de départ sont nécessaires pour le générateur de nombres aléatoire
536870986	L'objet existe déjà
536870987	Combinaison d'algorithme incorrecte. (Voir CBIRecrypt ( )).
536870988	Le module Cryptoki (PKCS#11) n'a pas été initialisé.
536870989	Le module Cryptoki (PKCS#11) a été initialisé.
536870990	Impossible de charger le module Cryptoki (PKCS#11).
536870991	Certificat introuvable
536870992	Non approuvé
536870993	Clé non valide
536870994	La clé ne peut pas être exportée.
536870995	L'algorithme spécifié n'est pas pris en charge temporairement.
536870996	Le mode de déchiffrement saisi n'est pas pris en charge.
536870997	Erreur de compilation GSENC.
536870998	Le format de requête de données n'est pas reconnu.
536870999	Le certificat n'a pas de clé privée.
536871000	Paramètre système incorrect.
536871001	Une opération est active.
536871002	Un certificat de la chaîne n'est pas correctement imbriqué.
536871003	La CRL n'a pas pu être remplacée.
536871004	Le code PIN de l'utilisateur a déjà été initialisé.
805306369	Vous ne disposez pas des droits permettant d'effectuer cette opération. Accès refusé.
805306370	Opération non valide

Identifiant de l'erreur	Affichage
805306371	Paramètre utilisé non valide
805306372	L'objet existe déjà
805306373	L'objet est introuvable.
805306374	Exception de la base de données
805306375	L'opération a été annulée par l'utilisateur
805306376	Le token n'est pas attribué à un utilisateur spécifique
805306377	Le token est attribué à plusieurs utilisateurs
805306378	Le token est introuvable dans la base de données
805306379	Le token a été supprimé et retiré de la base de données
805306380	Impossible d'identifier le token dans la base de données.
805306381	La stratégie est attribuée à un groupe de stratégies. Supprimez l'attribution avant de supprimer la stratégie.
805306382	La stratégie est attribuée à une OU. Supprimez d'abord l'attribution.
805306383	Le certificat n'est pas valide pour ce responsable.
805306384	Le certificat a expiré pour ce responsable.
805306385	Le responsable est introuvable dans la base de données.
805306386	Le responsable sélectionné n'est pas unique.
805306387	Le responsable est bloqué et ne peut pas être authentifié.
805306388	Le responsable n'est plus ou n'est pas encore valide.
805306389	Impossible d'autoriser le responsable - requête en dehors des heures de bureau.
805306390	Une partie responsable ne peut pas se supprimer.
805306391	Le responsable principal de la sécurité ne peut pas être supprimé car un second responsable principal de la sécurité est nécessaire pour une authentification supplémentaire.
805306392	Le responsable de la sécurité ne peut pas être supprimé car un second responsable de la sécurité est requis pour une authentification supplémentaire.
805306393	Le responsable de la vérification ne peut pas être supprimé car un second responsable de la vérification est requis pour une authentification supplémentaire.
805306394	Le responsable de la récupération ne peut pas être supprimé car un second responsable récupération est requis pour une authentification supplémentaire.
805306395	Le conseiller principal ne peut pas être supprimé car un second conseiller principal est requis pour une authentification supplémentaire.

Identifiant de l'erreur	Affichage
805306396	La fonction de responsable principal de la sécurité ne peut pas être supprimée car un second responsable principal de la sécurité est nécessaire pour une authentification supplémentaire.
805306397	La fonction de responsable de la sécurité ne peut pas être supprimée car un second responsable de la sécurité est nécessaire pour une authentification supplémentaire.
805306398	La fonction de responsable de la vérification ne peut pas être supprimée car un second responsable de la vérification est nécessaire pour une authentification supplémentaire.
805306399	La fonction de responsable récupération ne peut pas être supprimée car un second responsable récupération est nécessaire pour une authentification supplémentaire.
805306400	La fonction de responsable récupération ne peut pas être supprimée car un second responsable récupération est nécessaire pour une authentification supplémentaire.
805306401	Aucun responsable supplémentaire ayant la fonction requise n'est disponible pour une authentification supplémentaire.
805306402	Journal des événements
805306403	L'intégrité du journal des événements central a été vérifiée.
805306404	Intégrité rompue. Un ou plusieurs événements ont été supprimés du début de la chaîne.
805306405	Intégrité rompue. Un ou plusieurs événements ont été supprimés de la chaîne. Le message indiquant la détection du point de rupture de la chaîne a été mis en surbrillance.
805306406	Intégrité rompue. Un ou plusieurs événements ont été supprimés de la fin de la chaîne.
805306407	Impossible d'exporter les événements dans le fichier. Raison :
805306408	L'affichage actuel comprend des données non enregistrées. Voulez-vous enregistrer les modifications avant de quitter cet affichage?
805306409	Le fichier n'a pas pu être chargé ou est endommagé. Raison :
805306410	L'intégrité du journal a été rompue. Un ou plusieurs événements ont été supprimés.
805306411	Voulez-vous enregistrer les événements dans un fichier avant de les supprimer ?
805306412	Affichage des tâches
805306413	Plusieurs CRL trouvées dans la base de données : Impossible de supprimer les CRL.
805306414	CRL non trouvée dans la base de données :

Identifiant de l'erreur	Affichage
805306415	L'utilisateur auquel le certificat devrait avoir été attribué est introuvable dans la base de données.
805306416	Un blob P7 est requis en urgence pour l'attribution d'un certificat.
805306417	L'utilisateur auquel le certificat devrait avoir été attribué n'a pas un nom unique.
805306418	Il est malheureusement impossible de trouver l'attribution du certificat.
805306419	L'attribution du certificat n'est pas unique. Le certificat devant être supprimé n'est pas clair.
805306420	L'utilisateur pour lequel le certificat doit être produit est introuvable dans la base de données.
805306421	L'utilisateur auquel le certificat doit être attribué ne peut pas avoir un nom unique.
805306422	Le certificat a déjà été attribué à un autre utilisateur. Un certificat ne peut être attribué qu'à un seul utilisateur.
805306423	La machine à laquelle le certificat doit être attribué est introuvable dans la base de données.
805306424	La machine à laquelle le certificat doit être attribué n'a pas pu être identifiée de façon unique.
805306425	Les certificats importés ne peuvent pas être étendus par SGN.
805306426	Données de certificat incohérentes
805306427	L'extension du certificat n'a pas été approuvée par un responsable de la sécurité.
805306428	Erreur de suppression du token
805306429	Le certificat ne peut pas être supprimé par le token car il a été autorisé par l'utilisateur présent.
805306430	Un accès système du même nom existe déjà. Sélectionnez un autre nom.
805306431	Aucun rôle n'est affecté au responsable de la sécurité. La connexion est impossible.
805306432	La licence a été violée.
805306433	Aucune licence trouvée.
805306435	Chemin du fichier journal manquant ou incorrect.
2415919104	Aucune stratégie trouvée.
2415919105	Aucun fichier de configuration n'est disponible.
2415919106	Aucune connexion au serveur.
2415919107	Aucune donnée supplémentaire.

Identifiant de l'erreur	Affichage
2415919108	Priorité non valide utilisée pour l'envoi au serveur.
2415919109	Données supplémentaires en attente.
2415919110	Enregistrement automatique en attente.
2415919111	Échec de l'authentification de la base de données.
2415919112	Identifiant de session erroné.
2415919113	Paquet de données ignoré.
3674210305	Domaine introuvable.
3674210306	Machine introuvable.
3674210307	Utilisateur introuvable.
3758096385	Le mot de passe ne contient pas assez de lettres
3758096386	Le mot de passe ne contient pas assez de chiffres
3758096387	Le mot de passe ne contient pas assez de caractères spéciaux
3758096388	Le mot de passe est identique au nom d'utilisateur
3758096389	Le mot de passe contient des caractères consécutifs
3758096390	Le mot de passe ressemble trop au nom d'utilisateur
3758096391	Le mot de passe figure dans la liste des mots de passe interdits
3758096392	Le mot de passe ressemble trop à l'ancien mot de passe
3758096393	Le mot de passe comporte une séquence clavier de plus de deux caractères
3758096394	Le mot de passe comporte une colonne clavier de plus de deux caractères
3758096395	Le mot de passe n'est pas encore valide
3758096396	Un mot de passe a expiré
3758096397	La période de validité minimum du mot de passe n'est pas expirée
3758096398	La période de validité maximum du mot de passe est expirée
3758096399	Les informations concernant un changement de mot de passe imminent doivent être affichées
3758096400	Doit être changé lors de la première connexion
3758096401	Le mot de passe a été trouvé dans l'historique
3758096402	Erreur lors de la vérification par rapport à la liste noire spécifiée.
4026531840	Aucune "plate-forme" trouvée.
4026531841	Aucun document.

Identifiant de l'erreur	Affichage
4026531842	Erreur d'analyse XML.
4026531843	Erreur Document Object Model (XML).
4026531844	Aucune balise <DATAROOT> trouvée.
4026531845	Balise XML introuvable.
4026531846	Erreur "nostream".
4026531847	Erreur "printtree".

35.2 Codes d'erreur BitLocker

Les erreurs BitLocker sont signalées par les événements SafeGuard suivants :

- 2072 : échec de l'initialisation du noyau. Code interne : <*code d'erreur*>.
- 3506 : échec et clôture du chiffrement initial du secteur pour le lecteur <*lettre du lecteur*> . Raison : <*code d'erreur*>.

Le tableau suivant est une liste des codes d'erreur pour BitLocker :

Code d'erreur (Hex)	Code d'erreur (Déc)	Description
0x00000000 – 0x000032C8	0 – 15999	Veuillez consulter les Codes d'erreurs système de Microsoft
0x00BEB001	12496897	Chiffrement impossible en raison d'une erreur pendant l'initialisation du noyau.
0x00BEB002	12496898	Le gestionnaire de démarrage ne doit pas se trouver sur le volume du système à chiffrer.
0x00BEB003	12496899	Version de Windows non prise en charge sur le disque dur. La version minimum est Windows Vista.
0x00BEB004	12496900	La méthode d'authentification configuré n'est pas prise en charge.
0x00BEB005	12496901	La boîte de dialogue du code PIN ne s'est pas terminée correctement.
0x00BEB006	12496902	La boîte de dialogue de chemin d'accès ne s'est pas terminée correctement.
0x00BEB007	12496903	Erreur de communication entre processus dans la boîte de dialogue du code PIN ou de chemin d'accès.
0x00BEB008	12496904	Exception non prise en charge dans la boîte de dialogue du code PIN ou de chemin d'accès. La boîte de dialogue s'est affichée

		mais l'utilisateur s'est déconnecté ou l'a terminée à l'aide du Gestionnaire des tâches.
0x00BEB009	12496905	L'algorithme de chiffrement défini dans la stratégie ne correspond pas à celui du lecteur chiffré. Par défaut (s'il n'a pas été modifié), un volume BitLocker natif utilise AES-128 tandis que les stratégies SGN définissent AES-256.
0x00BEB102	12497154	La version UEFI n'a pas pu être validée et BitLocker va donc être exécuté en mode hérité.
0x00BEB202	12497410	Le package de configuration client n'a pas encore été installé.
0x00BEB203	12497411	La version UEFI n'est pas prise en charge et BitLocker va donc être exécuté en mode hérité. La configuration minimum requise est 2.3.1.
0x80280006	-2144862202	Module de plate-forme sécurisée inactif.
0x80280007	-2144862201	Module de plate-forme sécurisée désactivé.
0x80280014	-2144862188	Le module de plate-forme sécurisée a déjà un propriétaire.
0x80310037	-2144272329	Le paramètre de stratégie de groupe qui exige la compatibilité FIPS empêche la génération du mot de passe de récupération locale et son écriture sur le fichier de sauvegarde de la clé. Le chiffrement va tout de même se poursuivre.
0x8031005B	-2144272293	La stratégie de groupe pour la méthode d'authentification spécifiée n'est pas définie. Veuillez activer la stratégie de groupe "Demander une authentification supplémentaire au démarrage".
0x8031005E	-2144272290	La stratégie de groupe pour le chiffrement sans module de plate-forme sécurisée n'est pas définie. Veuillez activer la stratégie de groupe "Demander une authentification supplémentaire au démarrage" et sélectionner la case "Autoriser BitLocker sans un module de plateforme sécurisée compatible".
0x80280000 – 0x803100CF	-2144862208 – -2144272177	Veuillez consulter les Codes d'erreur COM (TPM, PLA, FVE) de Microsoft.

36 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur http://community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos à l'adresse http://www.sophos.com/fr-fr/support.aspx/.
- Téléchargez la documentation des produits à l'adresse http://www.sophos.com/fr-fr/support/documentation/.
- Envoyez un e-mail à support@sophos.fr, y compris le(s) numéro(s) de version du logiciel Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tous les messages d'erreur.

37 Mentions légales

Les informations de copyright des fournisseurs tiers sont disponibles dans le document *Disclaimer and Copyright for 3rd Party Software* dans votre répertoire des produits.